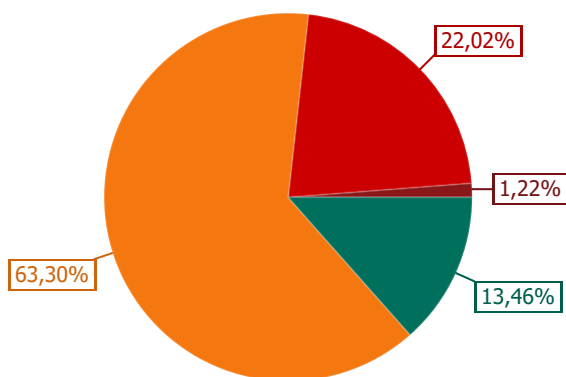


№ отчёта	af032e66-f7e5-4747-951c-833872bef9e1
Профиль	Уязвимости
Задание	уя-расписание
Начало/завершение сканирования	08.03.2023 14:40:25 / 08.03.2023 14:42:39
Формирование отчёта	22.03.2023 13:27:30
Имя	Quick_900
Описание	Автогенерируемый отчёт вкладки "История" для "mail" из "уя-расписание" задания.
Хосты [1]	mail

Диаграмма распределения уязвимостей по уровням риска


Риск	Количество
Критический	4
Высокий	72
Средний	207
Низкий	44
Всего	327

Таблица распределения уязвимостей по хостам

Хост / Риск	Критический	Высокий	Средний	Низкий	Всего
mail	4	72	207	44	327
Всего	4	72	207	44	327

Таблица распределения уязвимостей по продуктам

Продукт / Риск	Критический	Высокий	Средний	Низкий	Всего
сре:/o:centos:centos:7	4	72	207	44	327
Всего	4	72	207	44	327

Хост: mail

CPE	cpe:/o:centos:centos:7
Начало/завершение сканирования	08.03.2023 14:40:25 / 08.03.2023 14:42:39
Учётные данные	Имя профиля: SSH-RCScan Тип: Linux Sudo: Да
Метод получения данных	С использованием агента
Тип сканирования	Полное
Уязвимостей найдено	327: 4 72 207 44

Уязвимости [327]

Хост	ALTX ID	Риск	Название
mail	317797	Критический	Red Hat/CentOS -- уязвимость в ppp (CVE-2020-8597) cpe:/o:centos:centos:7 ppp (0:2.4.5-33.el7)
mail	358388	Критический	Red Hat/CentOS -- уязвимость в glib2 (CVE-2021-27219) cpe:/o:centos:centos:7 glib2 (0:2.56.1-5.el7)
mail	372948	Критический	Red Hat/CentOS -- уязвимость в nss, thunderbird (CVE-2021-43527) cpe:/o:centos:centos:7 nss (0:3.44.0-7.el7_7) nss-sysinit (0:3.44.0-7.el7_7) nss-tools (0:3.44.0-7.el7_7)
mail	383732	Критический	Red Hat/CentOS -- уязвимость в firefox, thunderbird, expat (CVE-2022-25236) cpe:/o:centos:centos:7 expat (0:2.1.0-10.el7_3)
mail	205829	Высокий	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2016-5131) cpe:/o:centos:centos:7 libxml2 (0:2.9.1-6.el7_2.3)
mail	207017	Высокий	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2017-15412) cpe:/o:centos:centos:7 libxml2 (0:2.9.1-6.el7_2.3)
mail	211012	Высокий	Red Hat -- уязвимость в expat (CVE-2015-2716) cpe:/o:centos:centos:7 expat (0:2.1.0-10.el7_3)
mail	291909	Высокий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-11487) cpe:/o:centos:centos:7 kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7) kernel-tools-libs (0:3.10.0-1062.9.1.el7) python-perf (0:3.10.0-1062.9.1.el7)
mail	295855	Высокий	Red Hat/CentOS -- уязвимость в thunderbird, expat (CVE-2019-15903) cpe:/o:centos:centos:7 expat (0:2.1.0-10.el7_3)
mail	311018	Высокий	Red Hat/CentOS -- уязвимость в chromium-browser, sqlite (CVE-2019-13734) cpe:/o:centos:centos:7 sqlite (0:3.7.17-8.el7)
mail	316323	Высокий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-14816) cpe:/o:centos:centos:7 kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7) kernel-tools-libs (0:3.10.0-1062.9.1.el7) python-perf (0:3.10.0-1062.9.1.el7)
mail	316325	Высокий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-14895) cpe:/o:centos:centos:7 kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7)

			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	316327	Высокий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-14901)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	316329	Высокий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-17133)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	316895	Высокий	Red Hat/CentOS -- уязвимость в sudo (CVE-2019-18634)
<i>cpe:/o:centos:centos:7</i>			<i>sudo (0:1.8.23-4.el7_7.1)</i>
mail	317766	Высокий	Red Hat/CentOS -- уязвимость в evolution-data-server, evolution, evolution-ews, atk (CVE-2019-3890)
<i>cpe:/o:centos:centos:7</i>			<i>atk (0:2.28.1-1.el7)</i>
mail	319001	Высокий	Red Hat/CentOS -- уязвимость в icu, nodejs (CVE-2020-10531)
<i>cpe:/o:centos:centos:7</i>			<i>libicu (0:50.2-3.el7)</i>
mail	320180	Высокий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-16746)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	325927	Высокий	Red Hat/CentOS -- уязвимость в Bind, bind-chroot, bind-devel, bind-libs, bind-libs-lite, bind-license, bind-lite-devel, bind-pkcs11, bind-pkcs11-devel, bind-pkcs11-libs, bind-pkcs11-utils, bind-sdb, bind-sdb-chroot, bind-utils, bind-debugsource, bind-export-devel, bind-export-libs, python3-bind (CVE-2020-8616)
<i>cpe:/o:centos:centos:7</i>			<i>bind-export-libs (32:9.11.4-9.P2.el7)</i>
			<i>bind-libs-lite (32:9.11.4-9.P2.el7)</i>
			<i>bind-license (32:9.11.4-9.P2.el7)</i>
mail	325928	Высокий	Red Hat/CentOS -- уязвимость в Bind, bind-chroot, bind-devel, bind-libs, bind-libs-lite, bind-license, bind-lite-devel, bind-pkcs11, bind-pkcs11-devel, bind-pkcs11-libs, bind-pkcs11-utils, bind-sdb, bind-sdb-chroot, bind-utils, bind-debugsource, bind-export-devel, bind-export-libs, python3-bind (CVE-2020-8617)
<i>cpe:/o:centos:centos:7</i>			<i>bind-export-libs (32:9.11.4-9.P2.el7)</i>
			<i>bind-libs-lite (32:9.11.4-9.P2.el7)</i>
			<i>bind-license (32:9.11.4-9.P2.el7)</i>
mail	330683	Высокий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19807)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	332426	Высокий	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-10713)
<i>cpe:/o:centos:centos:7</i>			<i>mokutil (0:15-2.el7.centos)</i>
			<i>shim-x64 (0:15-2.el7.centos)</i>
			<i>grub2-common (1:2.02-0.80.el7.centos)</i>

			<i>grub2-efi-x64 (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-extra (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-minimal (1:2.02-0.80.el7.centos)</i>
mail	333903	Высокий	Red Hat/CentOS -- уязвимость в nspr, nss, nss-sofotkn (CVE-2019-17006)
<i>cpe:/o:centos:centos:7</i>			<i>nspr (0:4.21.0-1.el7)</i>
			<i>nss (0:3.44.0-7.el7_7)</i>
			<i>nss-sofotkn (0:3.44.0-8.el7_7)</i>
			<i>nss-sofotkn-freebl (0:3.44.0-8.el7_7)</i>
			<i>nss-sysinit (0:3.44.0-7.el7_7)</i>
			<i>nss-tools (0:3.44.0-7.el7_7)</i>
			<i>nss-util (0:3.44.0-4.el7_7)</i>
mail	337352	Высокий	Red Hat/CentOS -- уязвимость в kernel (CVE-2019-19447)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337397	Высокий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-14305)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337768	Высокий	Red Hat/CentOS -- уязвимость в expat (CVE-2018-20843)
<i>cpe:/o:centos:centos:7</i>			<i>expat (0:2.1.0-10.el7_3)</i>
mail	337784	Высокий	Red Hat/CentOS -- уязвимость в libtiff (CVE-2019-17546)
<i>cpe:/o:centos:centos:7</i>			<i>libtiff (0:4.0.3-32.el7)</i>
mail	337794	Высокий	Red Hat/CentOS -- уязвимость в e2fsprogs (CVE-2019-5188)
<i>cpe:/o:centos:centos:7</i>			<i>e2fsprogs (0:1.42.9-16.el7)</i>
			<i>e2fsprogs-libs (0:1.42.9-16.el7)</i>
			<i>libcom_err (0:1.42.9-16.el7)</i>
			<i>libss (0:1.42.9-16.el7)</i>
mail	340349	Высокий	Red Hat/CentOS -- уязвимость в chromium-browser, freetype (CVE-2020-15999)
<i>cpe:/o:centos:centos:7</i>			<i>freetype (0:2.8-14.el7)</i>
mail	341389	Высокий	Red Hat/CentOS -- уязвимость в libx11, mesa, libdrm, libwacom, xorg-x11-drivers, egl-wayland, libglvnd, libinput (CVE-2020-14363)
<i>cpe:/o:centos:centos:7</i>			<i>libX11 (0:1.6.7-2.el7)</i>
			<i>libX11-common (0:1.6.7-2.el7)</i>
mail	343988	Высокий	Red Hat/CentOS -- уязвимость в linux-firmware, iwl1000-firmware, iwl100-firmware, iwl105-firmware, iwl135-firmware, iwl2000-firmware, iwl2030-firmware, iwl3160-firmware, iwl3945-firmware, iwl4965-firmware, iwl5000-firmware, iwl5150-firmware, iwl6000-firmware, iwl6000g2a-firmware, iwl6000g2b-firmware, iwl6050-firmware, iwl7260-firmware, libertas-sd8686-firmware, libertas-sd8787-firmware, libertas-usb8388-firmware, libertas-usb8388-olpc-firmware (CVE-2020-12321)
<i>cpe:/o:centos:centos:7</i>			<i>iwl100-firmware (0:39.31.5.1-72.el7)</i>
			<i>iwl1000-firmware (1:39.31.5.1-72.el7)</i>
			<i>iwl105-firmware (0:18.168.6.1-72.el7)</i>
			<i>iwl135-firmware (0:18.168.6.1-72.el7)</i>
			<i>iwl2000-firmware (0:18.168.6.1-72.el7)</i>
			<i>iwl2030-firmware (0:18.168.6.1-72.el7)</i>
			<i>iwl3160-firmware (0:22.0.7.0-72.el7)</i>

iwl3945-firmware (0:15.32.2.9-72.el7)
iwl4965-firmware (0:228.61.2.24-72.el7)
iwl5000-firmware (0:8.83.5.1_1-72.el7)
iwl5150-firmware (0:8.24.2.2-72.el7)
iwl6000-firmware (0:9.221.4.1-72.el7)
iwl6000g2a-firmware (0:17.168.5.3-72.el7)
iwl6000g2b-firmware (0:17.168.5.2-72.el7)
iwl6050-firmware (0:41.28.5.1-72.el7)
iwl7260-firmware (0:22.0.7.0-72.el7)
linux-firmware (0:20190429-72.gitd4de598.el7)

mail	346076	Высокий	Red Hat/CentOS -- уязвимость в sudo (CVE-2021-3156)
cpe:/o:centos:centos:7			sudo (0:1.8.23-4.el7_7.1)
mail	347611	Высокий	Red Hat/CentOS -- уязвимость в perl (CVE-2020-10543)
cpe:/o:centos:centos:7			perl (4:5.16.3-294.el7_6)
			perl-Pod-Escapes (1:1.04-294.el7_6)
			perl-libs (4:5.16.3-294.el7_6)
			perl-macros (4:5.16.3-294.el7_6)
mail	347612	Высокий	Red Hat/CentOS -- уязвимость в perl (CVE-2020-10878)
cpe:/o:centos:centos:7			perl (4:5.16.3-294.el7_6)
			perl-Pod-Escapes (1:1.04-294.el7_6)
			perl-libs (4:5.16.3-294.el7_6)
			perl-macros (4:5.16.3-294.el7_6)
mail	348240	Высокий	Red Hat/CentOS -- уязвимость в kernel (CVE-2020-29661)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	348949	Высокий	Red Hat/CentOS -- уязвимость в Bind (CVE-2020-8625)
cpe:/o:centos:centos:7			bind-export-libs (32:9.11.4-9.P2.el7)
			bind-libs-lite (32:9.11.4-9.P2.el7)
			bind-license (32:9.11.4-9.P2.el7)
mail	350027	Высокий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-25645)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	350030	Высокий	Red Hat/CentOS -- уязвимость в kernel (CVE-2020-28374)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	350449	Высокий	Red Hat/CentOS -- уязвимость в nettle (CVE-2021-20305)
cpe:/o:centos:centos:7			nettle (0:2.7.1-8.el7)

mail	350458	Высокий	Red Hat/CentOS -- уязвимость в kernel, kpatch-patch-4_18_0-193, kpatch-patch-4_18_0-193_1_2, kpatch-patch-4_18_0-193_6_3, kpatch-patch-4_18_0-193_13_2, kpatch-patch-4_18_0-193_14_3, kpatch-patch-4_18_0-193_19_1, kpatch-patch-4_18_0-193_28_1, kpatch-patch-4_18_0-193_29_1, kpatch-patch-4_18_0-193_37_1, kpatch-patch-4_18_0-193_40_1, kpatch-patch-4_18_0-193_41_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-3_10_0-957_54_1, kpatch-patch-3_10_0-957_56_1, kpatch-patch-3_10_0-957_58_2, kpatch-patch-3_10_0-957_61_1, kpatch-patch-3_10_0-957_61_2, kpatch-patch-3_10_0-957_62_1, kpatch-patch-3_10_0-957_65_1, kpatch-patch-3_10_0-957_66_1, kpatch-patch-3_10_0-957_70_1, kpatch-patch-3_10_0-1062_26_1 (CVE-2021-27365)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	359156	Высокий	Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-24489)
<i>cpe:/o:centos:centos:7</i>			<i>microcode_ctl (2:2.1-53.7.el7_7)</i>
mail	359165	Высокий	Red Hat/CentOS -- уязвимость в DHCP (CVE-2021-25217)
<i>cpe:/o:centos:centos:7</i>			<i>dhclient (12:4.2.5-77.el7.centos)</i>
			<i>dhcp-common (12:4.2.5-77.el7.centos)</i>
			<i>dhcp-libs (12:4.2.5-77.el7.centos)</i>
mail	361759	Высокий	Red Hat/CentOS -- уязвимость в kpatch-patch-4_18_0-305, kernel-rt, kernel, kpatch-patch-4_18_0-147_24_2, kpatch-patch-4_18_0-193_13_2, kpatch-patch-3_10_0-1160, kpatch-patch-3_10_0-1062_30_1, kpatch-patch-3_10_0-957_58_2 (CVE-2021-33034)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	364176	Высокий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2021-33033)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	364177	Высокий	Red Hat/CentOS -- уязвимость в kernel, kpatch-patch-4_18_0-193_13_2, kpatch-patch-3_10_0-1160, kpatch-patch-4_18_0-147_24_2, kpatch-patch-4_18_0-305, kernel-rt, kpatch-patch-3_10_0-1062_30_1, kpatch-patch-3_10_0-957_58_2 (CVE-2021-33909)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	365759	Высокий	Red Hat/CentOS -- уязвимость в kpatch-patch-3_10_0-1062_36_1, kernel, kpatch-patch-3_10_0-957_61_1, kernel-rt, kpatch-patch-4_18_0-193_19_1, kpatch-patch-3_10_0-1160, kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-305 (CVE-2021-22555)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	370722	Высокий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2021-3653)

cpe:/o:centos:centos:7

kernel (0:3.10.0-1062.9.1.el7)
kernel (0:3.10.0-514.el7)
kernel-tools (0:3.10.0-1062.9.1.el7)
kernel-tools-libs (0:3.10.0-1062.9.1.el7)
python-perf (0:3.10.0-1062.9.1.el7)

mail	370723	Высокий	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2021-3656)
cpe:/o:centos:centos:7			
kernel (0:3.10.0-1062.9.1.el7)			
kernel (0:3.10.0-514.el7)			
kernel-tools (0:3.10.0-1062.9.1.el7)			
kernel-tools-libs (0:3.10.0-1062.9.1.el7)			
python-perf (0:3.10.0-1062.9.1.el7)			
mail	370724	Высокий	Red Hat/CentOS -- уязвимость в kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-193_19_1, kernel, kpatch-patch-3_10_0-1160_11_1, kpatch-patch-3_10_0-957_61_1, kpatch-patch-3_10_0-1062_40_1 (CVE-2021-37576)
cpe:/o:centos:centos:7			
kernel (0:3.10.0-1062.9.1.el7)			
kernel (0:3.10.0-514.el7)			
kernel-tools (0:3.10.0-1062.9.1.el7)			
kernel-tools-libs (0:3.10.0-1062.9.1.el7)			
python-perf (0:3.10.0-1062.9.1.el7)			
mail	371484	Высокий	Red Hat/CentOS -- уязвимость в binutils, gcc-toolset-10-gcc, gcc-toolset-11-gcc, gcc-toolset-10-annobin, rust-toolset:rhel8, annobin, gcc-toolset-11-binutils, gcc-toolset-10-binutils, llvm-toolset:rhel8, gcc-toolset-11-annobin, gcc (CVE-2021-42574)
cpe:/o:centos:centos:7			
binutils (0:2.27-41.base.el7_7.1)			
mail	377414	Высокий	Red Hat/CentOS -- уязвимость в libx11 (CVE-2021-31535)
cpe:/o:centos:centos:7			
libX11 (0:1.6.7-2.el7)			
libX11-common (0:1.6.7-2.el7)			
mail	378727	Высокий	Red Hat/CentOS -- уязвимость в httpd:2.4, httpd (CVE-2021-26691)
cpe:/o:centos:centos:7			
httpd (0:2.4.6-90.el7.centos)			
httpd-tools (0:2.4.6-90.el7.centos)			
mail	378765	Высокий	Red Hat/CentOS -- уязвимость в httpd, httpd:2.4 (CVE-2021-40438)
cpe:/o:centos:centos:7			
httpd (0:2.4.6-90.el7.centos)			
httpd-tools (0:2.4.6-90.el7.centos)			
mail	379781	Высокий	Red Hat/CentOS -- уязвимость в httpd:2.4, httpd (CVE-2021-39275)
cpe:/o:centos:centos:7			
httpd (0:2.4.6-90.el7.centos)			
httpd-tools (0:2.4.6-90.el7.centos)			
mail	379793	Высокий	Red Hat/CentOS -- уязвимость в httpd:2.4, httpd (CVE-2021-44790)
cpe:/o:centos:centos:7			
httpd (0:2.4.6-90.el7.centos)			
httpd-tools (0:2.4.6-90.el7.centos)			
mail	380094	Высокий	Red Hat/CentOS -- уязвимость в polkit (CVE-2021-4034)
cpe:/o:centos:centos:7			
polkit (0:0.112-22.el7_7.1)			
mail	382894	Высокий	Red Hat/CentOS -- уязвимость в cyrus-sasl (CVE-2022-24407)
cpe:/o:centos:centos:7			
cyrus-sasl-lib (0:2.1.26-23.el7)			
mail	383731	Высокий	Red Hat/CentOS -- уязвимость в firefox, thunderbird, expat, xmlrpc-c (CVE-2022-25235)
cpe:/o:centos:centos:7			
expat (0:2.1.0-10.el7_3)			
mail	383733	Высокий	Red Hat/CentOS -- уязвимость в firefox, thunderbird, expat (CVE-2022-25315)
cpe:/o:centos:centos:7			
expat (0:2.1.0-10.el7_3)			
mail	384216	Высокий	Red Hat/CentOS -- уязвимость в expat (CVE-2021-45960)
cpe:/o:centos:centos:7			
expat (0:2.1.0-10.el7_3)			
mail	384217	Высокий	Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2021-46143)
cpe:/o:centos:centos:7			
expat (0:2.1.0-10.el7_3)			

mail	384219	Высокий	Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2022-22822)
cpe:/o:centos:centos:7			expat (0:2.1.0-10.el7_3)
mail	384220	Высокий	Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2022-22823)
cpe:/o:centos:centos:7			expat (0:2.1.0-10.el7_3)
mail	384221	Высокий	Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2022-22824)
cpe:/o:centos:centos:7			expat (0:2.1.0-10.el7_3)
mail	384222	Высокий	Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2022-22825)
cpe:/o:centos:centos:7			expat (0:2.1.0-10.el7_3)
mail	384223	Высокий	Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2022-22826)
cpe:/o:centos:centos:7			expat (0:2.1.0-10.el7_3)
mail	384224	Высокий	Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2022-22827)
cpe:/o:centos:centos:7			expat (0:2.1.0-10.el7_3)
mail	384225	Высокий	Red Hat/CentOS -- уязвимость в expat (CVE-2022-23852)
cpe:/o:centos:centos:7			expat (0:2.1.0-10.el7_3)
mail	387955	Высокий	Red Hat/CentOS -- уязвимость в OpenSSL, compat-openssl10, compat-openssl11 (CVE-2022-0778)
cpe:/o:centos:centos:7			openssl (1:1.0.2k-19.el7) openssl-lib (1:1.0.2k-19.el7)
mail	390363	Высокий	Red Hat/CentOS -- уязвимость в zlib, rsync (CVE-2018-25032)
cpe:/o:centos:centos:7			zlib (0:1.2.7-18.el7)
mail	404030	Высокий	Red Hat/CentOS -- уязвимость в systemd (CVE-2022-2526)
cpe:/o:centos:centos:7			libgudev1 (0:219-67.el7_7.2) systemd (0:219-67.el7_7.2) systemd-libs (0:219-67.el7_7.2) systemd-sysv (0:219-67.el7_7.2)
mail	410366	Высокий	Red Hat/CentOS -- уязвимость в expat, firefox, thunderbird, compat-expat1 (CVE-2022-40674)
cpe:/o:centos:centos:7			expat (0:2.1.0-10.el7_3)
mail	415511	Высокий	Red Hat/CentOS -- уязвимость в krb5 (CVE-2022-42898)
cpe:/o:centos:centos:7			krb5-libs (0:1.15.1-37.el7_7.2)
mail	419836	Высокий	Red Hat/CentOS -- уязвимость в libXpm (CVE-2022-4883)
cpe:/o:centos:centos:7			libXpm (0:3.5.12-1.el7)
mail	419838	Высокий	Red Hat/CentOS -- уязвимость в sudo (CVE-2023-22809)
cpe:/o:centos:centos:7			sudo (0:1.8.23-4.el7_7.1)
mail	421523	Высокий	Red Hat/CentOS -- уязвимость в WebKitGTK (CVE-2023-23529)
cpe:/o:centos:centos:7			
mail	286967	Средний	Red Hat/CentOS -- уязвимость в dbus (CVE-2019-12749)
cpe:/o:centos:centos:7			dbus (1:1.10.24-13.el7_6) dbus-libs (1:1.10.24-13.el7_6)
mail	288301	Средний	Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2019-11719)
cpe:/o:centos:centos:7			nspr (0:4.21.0-1.el7) nss (0:3.44.0-7.el7_7) nss-softokn (0:3.44.0-8.el7_7) nss-softokn-freebl (0:3.44.0-8.el7_7) nss-sysinit (0:3.44.0-7.el7_7) nss-tools (0:3.44.0-7.el7_7) nss-util (0:3.44.0-4.el7_7)
mail	289444	Средний	Red Hat/CentOS -- уязвимость в mariadb:10.3, mariadb, mariadb-devel, MySQL (CVE-2019-2737)
cpe:/o:centos:centos:7			mariadb (1:5.5.64-1.el7)

			<i>mariadb-libs (1:5.5.64-1.el7)</i> <i>mariadb-server (1:5.5.64-1.el7)</i>
mail	289446	Средний	Red Hat/CentOS -- уязвимость в mariadb:10.3, mariadb, mariadb-devel, MySQL (CVE-2019-2739)
<i>cpe:/o:centos:centos:7</i>			<i>mariadb (1:5.5.64-1.el7)</i>
			<i>mariadb-libs (1:5.5.64-1.el7)</i>
			<i>mariadb-server (1:5.5.64-1.el7)</i>
mail	289447	Средний	Red Hat/CentOS -- уязвимость в mariadb:10.3, mariadb, mariadb-devel, MySQL (CVE-2019-2740)
<i>cpe:/o:centos:centos:7</i>			<i>mariadb (1:5.5.64-1.el7)</i>
			<i>mariadb-libs (1:5.5.64-1.el7)</i>
			<i>mariadb-server (1:5.5.64-1.el7)</i>
mail	289466	Средний	Red Hat/CentOS -- уязвимость в mariadb:10.3, mariadb, mariadb-devel, MySQL (CVE-2019-2805)
<i>cpe:/o:centos:centos:7</i>			<i>mariadb (1:5.5.64-1.el7)</i>
			<i>mariadb-libs (1:5.5.64-1.el7)</i>
			<i>mariadb-server (1:5.5.64-1.el7)</i>
mail	291917	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-9503)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	307173	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2018-19985)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	307174	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel, perf, kernel-debug, kernel-debug-devel, kernel-devel, kernel-doc, kernel-headers, kernel-abi-whitelists, kernel-tools, kernel-tools-libs, kernel-tools-libs-devel, python-perf (CVE-2018-20169)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	307177	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-10207)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	307183	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-11884)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	307185	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-13233)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>

			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	307211	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-15916)
<i>cpe:/o:centos:centos:7</i>			
			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	316326	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-14898)
<i>cpe:/o:centos:centos:7</i>			
			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	316331	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2019-17666)
<i>cpe:/o:centos:centos:7</i>			
			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	316332	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2019-19338)
<i>cpe:/o:centos:centos:7</i>			
			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	317741	Средний	Red Hat/CentOS -- уязвимость в Bind (CVE-2018-5745)
<i>cpe:/o:centos:centos:7</i>			
			<i>bind-export-libs (32:9.11.4-9.P2.el7)</i>
			<i>bind-libs-lite (32:9.11.4-9.P2.el7)</i>
			<i>bind-license (32:9.11.4-9.P2.el7)</i>
mail	317751	Средний	Red Hat/CentOS -- уязвимость в glib2, ibus (CVE-2019-12450)
<i>cpe:/o:centos:centos:7</i>			
			<i>glib2 (0:2.56.1-5.el7)</i>
mail	317763	Средний	Red Hat/CentOS -- уязвимость в dovecot (CVE-2019-3814)
<i>cpe:/o:centos:centos:7</i>			
			<i>dovecot (1:2.2.36-3.el7_7.1)</i>
			<i>dovecot-mysql (1:2.2.36-3.el7_7.1)</i>
			<i>dovecot-pigeonhole (1:2.2.36-3.el7_7.1)</i>
mail	320064	Средний	Red Hat/CentOS -- уязвимость в httpd (CVE-2017-15710)
<i>cpe:/o:centos:centos:7</i>			
			<i>httpd (0:2.4.6-90.el7.centos)</i>
			<i>httpd-tools (0:2.4.6-90.el7.centos)</i>
mail	320072	Средний	Red Hat/CentOS -- уязвимость в avahi (CVE-2017-6519)
<i>cpe:/o:centos:centos:7</i>			
			<i>avahi-libs (0:0.6.31-19.el7)</i>
mail	320078	Средний	Red Hat/CentOS -- уязвимость в file, file-devel, file-libs, file-static, python-magic (CVE-2018-10360)
<i>cpe:/o:centos:centos:7</i>			
			<i>file (0:5.11-35.el7)</i>
			<i>file-libs (0:5.11-35.el7)</i>
mail	320079	Средний	Red Hat/CentOS -- уязвимость в php (CVE-2018-10547)
<i>cpe:/o:centos:centos:7</i>			
			<i>php (0:5.4.16-46.1.el7_7)</i>
			<i>php-bcmath (0:5.4.16-46.1.el7_7)</i>
			<i>php-cli (0:5.4.16-46.1.el7_7)</i>
			<i>php-common (0:5.4.16-46.1.el7_7)</i>

php-intl (0:5.4.16-46.1.el7_7)
php-ldap (0:5.4.16-46.1.el7_7)
php-mbstring (0:5.4.16-46.1.el7_7)
php-mysql (0:5.4.16-46.1.el7_7)
php-pdo (0:5.4.16-46.1.el7_7)
php-process (0:5.4.16-46.1.el7_7)
php-xml (0:5.4.16-46.1.el7_7)
php-gd (0:5.4.16-46.1.el7_7)

mail	320098	Средний	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2018-14404)
<i>cpe:/o:centos:centos:7</i>			<i>libxml2 (0:2.9.1-6.el7_2.3)</i>
mail	320103	Средний	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2018-14567)
<i>cpe:/o:centos:centos:7</i>			<i>libxml2 (0:2.9.1-6.el7_2.3)</i>
mail	320104	Средний	Red Hat/CentOS -- уязвимость в evolution-data-server, evolution, atk, evolution-ews (CVE-2018-15587)
<i>cpe:/o:centos:centos:7</i>			<i>atk (0:2.28.1-1.el7)</i>
mail	320110	Средний	Red Hat/CentOS -- уязвимость в httpd, httpd:2.4 (CVE-2018-17199)
<i>cpe:/o:centos:centos:7</i>			<i>httpd (0:2.4.6-90.el7.centos)</i> <i>httpd-tools (0:2.4.6-90.el7.centos)</i>
mail	320118	Средний	Red Hat/CentOS -- уязвимость в python3, Python, python27 (CVE-2018-20852)
<i>cpe:/o:centos:centos:7</i>			<i>python (0:2.7.5-86.el7)</i> <i>python-libs (0:2.7.5-86.el7)</i>
mail	320120	Средний	Red Hat/CentOS -- уязвимость в cups (CVE-2018-4180)
<i>cpe:/o:centos:centos:7</i>			<i>cups-libs (1:1.6.3-40.el7)</i>
mail	320121	Средний	Red Hat/CentOS -- уязвимость в cups (CVE-2018-4181)
<i>cpe:/o:centos:centos:7</i>			<i>cups-libs (1:1.6.3-40.el7)</i>
mail	320122	Средний	Red Hat/CentOS -- уязвимость в cups (CVE-2018-4700)
<i>cpe:/o:centos:centos:7</i>			<i>cups-libs (1:1.6.3-40.el7)</i>
mail	320123	Средний	Red Hat/CentOS -- уязвимость в php (CVE-2018-5712)
<i>cpe:/o:centos:centos:7</i>			<i>php (0:5.4.16-46.1.el7_7)</i> <i>php-bcmath (0:5.4.16-46.1.el7_7)</i> <i>php-cli (0:5.4.16-46.1.el7_7)</i> <i>php-common (0:5.4.16-46.1.el7_7)</i> <i>php-intl (0:5.4.16-46.1.el7_7)</i> <i>php-ldap (0:5.4.16-46.1.el7_7)</i> <i>php-mbstring (0:5.4.16-46.1.el7_7)</i> <i>php-mysql (0:5.4.16-46.1.el7_7)</i> <i>php-pdo (0:5.4.16-46.1.el7_7)</i> <i>php-process (0:5.4.16-46.1.el7_7)</i> <i>php-xml (0:5.4.16-46.1.el7_7)</i> <i>php-gd (0:5.4.16-46.1.el7_7)</i>
mail	320124	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2018-7191)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i> <i>kernel (0:3.10.0-514.el7)</i> <i>kernel-tools (0:3.10.0-1062.9.1.el7)</i> <i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i> <i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	320126	Средний	Red Hat/CentOS -- уязвимость в php (CVE-2018-7584)
<i>cpe:/o:centos:centos:7</i>			<i>php (0:5.4.16-46.1.el7_7)</i> <i>php-bcmath (0:5.4.16-46.1.el7_7)</i> <i>php-cli (0:5.4.16-46.1.el7_7)</i> <i>php-common (0:5.4.16-46.1.el7_7)</i>

			<i>php-intl (0:5.4.16-46.1.el7_7)</i>
			<i>php-ldap (0:5.4.16-46.1.el7_7)</i>
			<i>php-mbstring (0:5.4.16-46.1.el7_7)</i>
			<i>php-mysql (0:5.4.16-46.1.el7_7)</i>
			<i>php-pdo (0:5.4.16-46.1.el7_7)</i>
			<i>php-process (0:5.4.16-46.1.el7_7)</i>
			<i>php-xml (0:5.4.16-46.1.el7_7)</i>
			<i>php-gd (0:5.4.16-46.1.el7_7)</i>
mail	320139	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-12382)
<i>cpe:/o:centos:centos:7</i>			
			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	320163	Средний	Red Hat/CentOS -- уязвимость в kernel, bpftool (CVE-2019-13648)
<i>cpe:/o:centos:centos:7</i>			
			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	320164	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-14283)
<i>cpe:/o:centos:centos:7</i>			
			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	320172	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-15221)
<i>cpe:/o:centos:centos:7</i>			
			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	320173	Средний	Red Hat/CentOS -- уязвимость в python3, Python, python27 (CVE-2019-16056)
<i>cpe:/o:centos:centos:7</i>			
			<i>python (0:2.7.5-86.el7)</i>
			<i>python-libs (0:2.7.5-86.el7)</i>
mail	320181	Средний	Red Hat/CentOS -- уязвимость в Rsyslog (CVE-2019-17041)
<i>cpe:/o:centos:centos:7</i>			
			<i>rsyslog (0:8.24.0-41.el7_7.2)</i>
mail	320182	Средний	Red Hat/CentOS -- уязвимость в Rsyslog (CVE-2019-17042)
<i>cpe:/o:centos:centos:7</i>			
			<i>rsyslog (0:8.24.0-41.el7_7.2)</i>
mail	320186	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2019-18660)
<i>cpe:/o:centos:centos:7</i>			
			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	320189	Средний	Red Hat/CentOS -- уязвимость в gnome (CVE-2019-3820)
<i>cpe:/o:centos:centos:7</i>			
			<i>colord-libs (0:1.3.4-1.el7)</i>
			<i>gsettings-desktop-schemas (0:3.28.0-2.el7)</i>
			<i>gtk-update-icon-cache (0:3.22.30-3.el7)</i>
			<i>gtk3 (0:3.22.30-3.el7)</i>
			<i>shared-mime-info (0:1.8-4.el7)</i>

mail	320190	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-3901)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	320191	Средний	Red Hat/CentOS -- уязвимость в curl, Libcurl (CVE-2019-5436)
cpe:/o:centos:centos:7			curl (0:7.29.0-54.el7_7.1)
			libcurl (0:7.29.0-54.el7_7.1)
mail	320192	Средний	Red Hat/CentOS -- уязвимость в Bind (CVE-2019-6477)
cpe:/o:centos:centos:7			bind-export-libs (32:9.11.4-9.P2.el7)
			bind-libs-lite (32:9.11.4-9.P2.el7)
			bind-license (32:9.11.4-9.P2.el7)
mail	320196	Средний	Red Hat/CentOS -- уязвимость в dovecot (CVE-2019-7524)
cpe:/o:centos:centos:7			dovecot (1:2.2.36-3.el7_7.1)
			dovecot-mysql (1:2.2.36-3.el7_7.1)
			dovecot-pigeonhole (1:2.2.36-3.el7_7.1)
mail	320197	Средний	Red Hat/CentOS -- уязвимость в php (CVE-2019-9024)
cpe:/o:centos:centos:7			php (0:5.4.16-46.1.el7_7)
			php-bcmath (0:5.4.16-46.1.el7_7)
			php-cli (0:5.4.16-46.1.el7_7)
			php-common (0:5.4.16-46.1.el7_7)
			php-intl (0:5.4.16-46.1.el7_7)
			php-ldap (0:5.4.16-46.1.el7_7)
			php-mbstring (0:5.4.16-46.1.el7_7)
			php-mysql (0:5.4.16-46.1.el7_7)
			php-pdo (0:5.4.16-46.1.el7_7)
			php-process (0:5.4.16-46.1.el7_7)
			php-xml (0:5.4.16-46.1.el7_7)
			php-gd (0:5.4.16-46.1.el7_7)
mail	320206	Средний	Red Hat/CentOS -- уязвимость в bash (CVE-2019-9924)
cpe:/o:centos:centos:7			bash (0:4.2.46-33.el7)
mail	321554	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19527)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	323683	Средний	Red Hat/CentOS -- уязвимость в glib2, ibus (CVE-2019-14822)
cpe:/o:centos:centos:7			glib2 (0:2.56.1-5.el7)
mail	323693	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19534)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	323700	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-1749)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)

			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	324169	Средний	Red Hat/CentOS -- уязвимость в e2fsprogs (CVE-2019-5094)
	<i>cpe:/o:centos:centos:7</i>		<i>e2fsprogs (0:1.42.9-16.el7)</i>
			<i>e2fsprogs-libs (0:1.42.9-16.el7)</i>
			<i>libcom_err (0:1.42.9-16.el7)</i>
			<i>libss (0:1.42.9-16.el7)</i>
mail	324171	Средний	Red Hat/CentOS -- уязвимость в curl (CVE-2019-5482)
	<i>cpe:/o:centos:centos:7</i>		<i>curl (0:7.29.0-54.el7_7.1)</i>
			<i>libcurl (0:7.29.0-54.el7_7.1)</i>
mail	324776	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-2732)
	<i>cpe:/o:centos:centos:7</i>		<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	326423	Средний	Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-0543)
	<i>cpe:/o:centos:centos:7</i>		<i>microcode_ctl (2:2.1-53.7.el7_7)</i>
mail	326425	Средний	Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-0549)
	<i>cpe:/o:centos:centos:7</i>		<i>microcode_ctl (2:2.1-53.7.el7_7)</i>
mail	327659	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt, kernel-rt-debug, kernel-rt-debug-devel, kernel-rt-devel, kernel-rt-doc, kernel-rt-trace, kernel-rt-trace-devel, bpftool (CVE-2020-12888)
	<i>cpe:/o:centos:centos:7</i>		<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	329835	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-12653)
	<i>cpe:/o:centos:centos:7</i>		<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	329836	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-12654)
	<i>cpe:/o:centos:centos:7</i>		<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	330685	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10757)
	<i>cpe:/o:centos:centos:7</i>		<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	330691	Средний	Red Hat/CentOS -- уязвимость в dbus (CVE-2020-12049)
	<i>cpe:/o:centos:centos:7</i>		<i>dbus (1:1.10.24-13.el7_6)</i>
			<i>dbus-libs (1:1.10.24-13.el7_6)</i>
mail	332428	Средний	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-14308)
	<i>cpe:/o:centos:centos:7</i>		<i>mokutil (0:15-2.el7.centos)</i>
			<i>shim-x64 (0:15-2.el7.centos)</i>

			<i>grub2-common (1:2.02-0.80.el7.centos)</i>
			<i>grub2-efi-x64 (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-extra (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-minimal (1:2.02-0.80.el7.centos)</i>
mail	332429	Средний	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-14309)
<i>cpe:/o:centos:centos:7</i>			<i>mokutil (0:15-2.el7.centos)</i>
			<i>shim-x64 (0:15-2.el7.centos)</i>
			<i>grub2-common (1:2.02-0.80.el7.centos)</i>
			<i>grub2-efi-x64 (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-extra (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-minimal (1:2.02-0.80.el7.centos)</i>
mail	332430	Средний	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-14310)
<i>cpe:/o:centos:centos:7</i>			<i>mokutil (0:15-2.el7.centos)</i>
			<i>shim-x64 (0:15-2.el7.centos)</i>
			<i>grub2-common (1:2.02-0.80.el7.centos)</i>
			<i>grub2-efi-x64 (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-extra (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-minimal (1:2.02-0.80.el7.centos)</i>
mail	332431	Средний	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-14311)
<i>cpe:/o:centos:centos:7</i>			<i>mokutil (0:15-2.el7.centos)</i>
			<i>shim-x64 (0:15-2.el7.centos)</i>
			<i>grub2-common (1:2.02-0.80.el7.centos)</i>
			<i>grub2-efi-x64 (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-extra (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-minimal (1:2.02-0.80.el7.centos)</i>
mail	332434	Средний	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-15705)
<i>cpe:/o:centos:centos:7</i>			<i>mokutil (0:15-2.el7.centos)</i>
			<i>shim-x64 (0:15-2.el7.centos)</i>
			<i>grub2-common (1:2.02-0.80.el7.centos)</i>
			<i>grub2-efi-x64 (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-extra (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-minimal (1:2.02-0.80.el7.centos)</i>
mail	332435	Средний	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-15706)
<i>cpe:/o:centos:centos:7</i>			<i>mokutil (0:15-2.el7.centos)</i>
			<i>shim-x64 (0:15-2.el7.centos)</i>
			<i>grub2-common (1:2.02-0.80.el7.centos)</i>
			<i>grub2-efi-x64 (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-extra (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-minimal (1:2.02-0.80.el7.centos)</i>
mail	332436	Средний	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-15707)
<i>cpe:/o:centos:centos:7</i>			<i>mokutil (0:15-2.el7.centos)</i>
			<i>shim-x64 (0:15-2.el7.centos)</i>
			<i>grub2-common (1:2.02-0.80.el7.centos)</i>
			<i>grub2-efi-x64 (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools (1:2.02-0.80.el7.centos)</i>

			<i>grub2-tools-extra (1:2.02-0.80.el7.centos)</i>
			<i>grub2-tools-minimal (1:2.02-0.80.el7.centos)</i>
mail	333902	Средний	Red Hat/CentOS -- уязвимость в nspr, nss, nss-softokn (CVE-2019-11756)
<i>cpe:/o:centos:centos:7</i>			
			<i>nspr (0:4.21.0-1.el7)</i>
			<i>nss (0:3.44.0-7.el7_7)</i>
			<i>nss-softokn (0:3.44.0-8.el7_7)</i>
			<i>nss-softokn-freebl (0:3.44.0-8.el7_7)</i>
			<i>nss-sysinit (0:3.44.0-7.el7_7)</i>
			<i>nss-tools (0:3.44.0-7.el7_7)</i>
			<i>nss-util (0:3.44.0-4.el7_7)</i>
mail	333904	Средний	Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2019-17023)
<i>cpe:/o:centos:centos:7</i>			
			<i>nspr (0:4.21.0-1.el7)</i>
			<i>nss (0:3.44.0-7.el7_7)</i>
			<i>nss-softokn (0:3.44.0-8.el7_7)</i>
			<i>nss-softokn-freebl (0:3.44.0-8.el7_7)</i>
			<i>nss-sysinit (0:3.44.0-7.el7_7)</i>
			<i>nss-tools (0:3.44.0-7.el7_7)</i>
			<i>nss-util (0:3.44.0-4.el7_7)</i>
mail	335564	Средний	Red Hat/CentOS -- уязвимость в dovecot (CVE-2020-12100)
<i>cpe:/o:centos:centos:7</i>			
			<i>dovecot (1:2.2.36-3.el7_7.1)</i>
			<i>dovecot-mysql (1:2.2.36-3.el7_7.1)</i>
			<i>dovecot-pigeonhole (1:2.2.36-3.el7_7.1)</i>
mail	335565	Средний	Red Hat/CentOS -- уязвимость в dovecot (CVE-2020-12673)
<i>cpe:/o:centos:centos:7</i>			
			<i>dovecot (1:2.2.36-3.el7_7.1)</i>
			<i>dovecot-mysql (1:2.2.36-3.el7_7.1)</i>
			<i>dovecot-pigeonhole (1:2.2.36-3.el7_7.1)</i>
mail	335566	Средний	Red Hat/CentOS -- уязвимость в dovecot (CVE-2020-12674)
<i>cpe:/o:centos:centos:7</i>			
			<i>dovecot (1:2.2.36-3.el7_7.1)</i>
			<i>dovecot-mysql (1:2.2.36-3.el7_7.1)</i>
			<i>dovecot-pigeonhole (1:2.2.36-3.el7_7.1)</i>
mail	336285	Средний	Red Hat/CentOS -- уязвимость в libcroco (CVE-2020-12825)
<i>cpe:/o:centos:centos:7</i>			
			<i>libcroco (0:0.6.12-4.el7)</i>
mail	336583	Средний	Red Hat/CentOS -- уязвимость в mysql:8.0, mariadb:10.3, mariadb, MySQL (CVE-2019-2974)
<i>cpe:/o:centos:centos:7</i>			
			<i>mariadb (1:5.5.64-1.el7)</i>
			<i>mariadb-libs (1:5.5.64-1.el7)</i>
			<i>mariadb-server (1:5.5.64-1.el7)</i>
mail	336629	Средний	Red Hat/CentOS -- уязвимость в mysql:8.0, mariadb-connector-c, mariadb:10.3, mariadb, MySQL (CVE-2020-2574)
<i>cpe:/o:centos:centos:7</i>			
			<i>mariadb (1:5.5.64-1.el7)</i>
			<i>mariadb-libs (1:5.5.64-1.el7)</i>
			<i>mariadb-server (1:5.5.64-1.el7)</i>
mail	336641	Средний	Red Hat/CentOS -- уязвимость в mysql:8.0, mariadb-connector-c, mariadb:10.3, mariadb, MySQL (CVE-2020-2752)
<i>cpe:/o:centos:centos:7</i>			
			<i>mariadb (1:5.5.64-1.el7)</i>
			<i>mariadb-libs (1:5.5.64-1.el7)</i>
			<i>mariadb-server (1:5.5.64-1.el7)</i>
mail	336651	Средний	Red Hat/CentOS -- уязвимость в mysql:8.0, mariadb:10.3, mariadb, MySQL (CVE-2020-2780)
<i>cpe:/o:centos:centos:7</i>			
			<i>mariadb (1:5.5.64-1.el7)</i>
			<i>mariadb-libs (1:5.5.64-1.el7)</i>
			<i>mariadb-server (1:5.5.64-1.el7)</i>

mail	336653	Средний	Red Hat/CentOS -- уязвимость в mysql:8.0, mariadb:10.3, mariadb, MySQL (CVE-2020-2812)
cpe:/o:centos:centos:7			mariadb (1:5.5.64-1.el7) mariadb-libs (1:5.5.64-1.el7) mariadb-server (1:5.5.64-1.el7)
mail	337335	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2017-18551)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7) kernel-tools-libs (0:3.10.0-1062.9.1.el7) python-perf (0:3.10.0-1062.9.1.el7)
mail	337336	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2018-20836)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7) kernel-tools-libs (0:3.10.0-1062.9.1.el7) python-perf (0:3.10.0-1062.9.1.el7)
mail	337338	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-15217)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7) kernel-tools-libs (0:3.10.0-1062.9.1.el7) python-perf (0:3.10.0-1062.9.1.el7)
mail	337339	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-15807)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7) kernel-tools-libs (0:3.10.0-1062.9.1.el7) python-perf (0:3.10.0-1062.9.1.el7)
mail	337340	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2019-15917)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7) kernel-tools-libs (0:3.10.0-1062.9.1.el7) python-perf (0:3.10.0-1062.9.1.el7)
mail	337343	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-16994)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7) kernel-tools-libs (0:3.10.0-1062.9.1.el7) python-perf (0:3.10.0-1062.9.1.el7)
mail	337344	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-18808)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7) kernel-tools-libs (0:3.10.0-1062.9.1.el7) python-perf (0:3.10.0-1062.9.1.el7)
mail	337345	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2019-19046)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7)

kernel-tools-libs (0:3.10.0-1062.9.1.el7)

python-perf (0:3.10.0-1062.9.1.el7)

mail	337346	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19055)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337347	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19058)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337348	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19059)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337349	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19062)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337350	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19063)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337351	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19332)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337353	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19523)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337354	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19524)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337355	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19530)

<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337357	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19767)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337358	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-20054)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337359	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-20095)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337360	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2019-20636)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337361	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2019-9454)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337362	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-9458)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337363	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10690)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337365	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10742)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>

			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337366	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10751)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337368	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10942)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337392	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-11565)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337393	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2020-12770)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337394	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-12826)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337404	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2020-8647)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337405	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2020-8649)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337406	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-9383)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337757	Средний	Red Hat/CentOS -- уязвимость в cups (CVE-2017-18190)

<i>cpe:/o:centos:centos:7</i>			<i>cups-libs (1:1.6.3-40.el7)</i>
mail	337759	Средний	Red Hat/CentOS -- уязвимость в httpd (CVE-2018-1283)
<i>cpe:/o:centos:centos:7</i>			<i>httpd (0:2.4.6-90.el7.centos)</i>
			<i>httpd-tools (0:2.4.6-90.el7.centos)</i>
mail	337760	Средний	Red Hat/CentOS -- уязвимость в httpd (CVE-2018-1303)
<i>cpe:/o:centos:centos:7</i>			<i>httpd (0:2.4.6-90.el7.centos)</i>
			<i>httpd-tools (0:2.4.6-90.el7.centos)</i>
mail	337777	Средний	Red Hat/CentOS -- уязвимость в cpio (CVE-2019-14866)
<i>cpe:/o:centos:centos:7</i>			<i>cpio (0:2.11-27.el7)</i>
mail	337779	Средний	Red Hat/CentOS -- уязвимость в python3 (CVE-2019-16935)
<i>cpe:/o:centos:centos:7</i>			<i>python (0:2.7.5-86.el7)</i>
			<i>python-libs (0:2.7.5-86.el7)</i>
mail	337783	Средний	Red Hat/CentOS -- уязвимость в libssh2 (CVE-2019-17498)
<i>cpe:/o:centos:centos:7</i>			<i>libssh2 (0:1.8.0-3.el7)</i>
mail	337787	Средний	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2019-19956)
<i>cpe:/o:centos:centos:7</i>			<i>libxml2 (0:2.9.1-6.el7_2.3)</i>
mail	337789	Средний	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2019-20388)
<i>cpe:/o:centos:centos:7</i>			<i>libxml2 (0:2.9.1-6.el7_2.3)</i>
mail	337911	Средний	Red Hat/CentOS -- уязвимость в openldap (CVE-2020-12243)
<i>cpe:/o:centos:centos:7</i>			<i>openldap (0:2.4.44-21.el7_6)</i>
mail	337914	Средний	Red Hat/CentOS -- уязвимость в nspr, nss, nss-softokn (CVE-2020-12403)
<i>cpe:/o:centos:centos:7</i>			<i>nspr (0:4.21.0-1.el7)</i>
			<i>nss (0:3.44.0-7.el7_7)</i>
			<i>nss-softokn (0:3.44.0-8.el7_7)</i>
			<i>nss-softokn-freebl (0:3.44.0-8.el7_7)</i>
			<i>nss-sysinit (0:3.44.0-7.el7_7)</i>
			<i>nss-tools (0:3.44.0-7.el7_7)</i>
			<i>nss-util (0:3.44.0-4.el7_7)</i>
mail	337931	Средний	Red Hat/CentOS -- уязвимость в httpd:2.4 (CVE-2020-1927)
<i>cpe:/o:centos:centos:7</i>			<i>httpd (0:2.4.6-90.el7.centos)</i>
			<i>httpd-tools (0:2.4.6-90.el7.centos)</i>
mail	337979	Средний	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2020-7595)
<i>cpe:/o:centos:centos:7</i>			<i>libxml2 (0:2.9.1-6.el7_2.3)</i>
mail	337981	Средний	Red Hat/CentOS -- уязвимость в Bind (CVE-2020-8622)
<i>cpe:/o:centos:centos:7</i>			<i>bind-export-libs (32:9.11.4-9.P2.el7)</i>
			<i>bind-libs-lite (32:9.11.4-9.P2.el7)</i>
			<i>bind-license (32:9.11.4-9.P2.el7)</i>
mail	339336	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2020-14331)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	339337	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt, kpatch-patch (CVE-2020-14385)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>

mail	341338	Средний	Red Hat/CentOS -- уязвимость в python38:3.8, python3, python27:2.7, Python (CVE-2019-20907)
cpe:/o:centos:centos:7			python (0:2.7.5-86.el7)
			python-libs (0:2.7.5-86.el7)
mail	341348	Средний	Red Hat/CentOS -- уязвимость в glibc (CVE-2020-10029)
cpe:/o:centos:centos:7			glibc (0:2.17-292.el7)
			glibc-common (0:2.17-292.el7)
mail	341363	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-11668)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	341419	Средний	Red Hat/CentOS -- уязвимость в curl (CVE-2020-8177)
cpe:/o:centos:centos:7			curl (0:7.29.0-54.el7_7.1)
			libcurl (0:7.29.0-54.el7_7.1)
mail	341421	Средний	Red Hat/CentOS -- уязвимость в Bind (CVE-2020-8623)
cpe:/o:centos:centos:7			bind-export-libs (32:9.11.4-9.P2.el7)
			bind-libs-lite (32:9.11.4-9.P2.el7)
			bind-license (32:9.11.4-9.P2.el7)
mail	341423	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2020-8648)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	341424	Средний	Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-8695)
cpe:/o:centos:centos:7			microcode_ctl (2:2.1-53.7.el7_7)
mail	341426	Средний	Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-8698)
cpe:/o:centos:centos:7			microcode_ctl (2:2.1-53.7.el7_7)
mail	343984	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-18282)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	343987	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10769)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	343991	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-14314)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	344005	Средний	Red Hat/CentOS -- уязвимость в OpenSSL (CVE-2020-1971)
cpe:/o:centos:centos:7			openssl (1:1.0.2k-19.el7)
			openssl-libs (1:1.0.2k-19.el7)

mail	344006	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-24394)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	344009	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-25212)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	344010	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-25643)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	344758	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2020-25211)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	347610	Средний	Red Hat/CentOS -- уязвимость в glibc (CVE-2019-25013)
cpe:/o:centos:centos:7			glibc (0:2.17-292.el7)
			glibc-common (0:2.17-292.el7)
mail	347613	Средний	Red Hat/CentOS -- уязвимость в perl (CVE-2020-12723)
cpe:/o:centos:centos:7			perl (4:5.16.3-294.el7_6)
			perl-Pod-Escapes (1:1.04-294.el7_6)
			perl-libs (4:5.16.3-294.el7_6)
			perl-macros (4:5.16.3-294.el7_6)
mail	347617	Средний	Red Hat/CentOS -- уязвимость в glibc (CVE-2020-29573)
cpe:/o:centos:centos:7			glibc (0:2.17-292.el7)
			glibc-common (0:2.17-292.el7)
mail	348237	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-14351)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	348239	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2020-25705)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	349343	Средний	Red Hat/CentOS -- уязвимость в wpa_supplicant (CVE-2021-27803)
cpe:/o:centos:centos:7			wpa_supplicant (1:2.6-12.el7)
mail	350025	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2019-19532)

<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	350026	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-0427)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	350031	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-7053)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	350033	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2021-20265)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	350443	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt, kpatch-patch-3_10_0-1062_46_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_70_1, kpatch-patch-4_18_0-147_20_1, kpatch-patch-4_18_0-193_13_2 (CVE-2020-0466)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	350456	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2021-27363)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	350457	Средний	Red Hat/CentOS -- уязвимость в kernel, kpatch-patch-4_18_0-193, kpatch-patch-4_18_0-193_1_2, kpatch-patch-4_18_0-193_6_3, kpatch-patch-4_18_0-193_13_2, kpatch-patch-4_18_0-193_14_3, kpatch-patch-4_18_0-193_19_1, kpatch-patch-4_18_0-193_28_1, kpatch-patch-4_18_0-193_29_1, kpatch-patch-4_18_0-193_37_1, kpatch-patch-4_18_0-193_40_1, kpatch-patch-4_18_0-193_41_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-3_10_0-957_54_1, kpatch-patch-3_10_0-957_56_1, kpatch-patch-3_10_0-957_58_2, kpatch-patch-3_10_0-957_61_1, kpatch-patch-3_10_0-957_61_2, kpatch-patch-3_10_0-957_62_1, kpatch-patch-3_10_0-957_65_1, kpatch-patch-3_10_0-957_66_1, kpatch-patch-3_10_0-957_70_1, kpatch-patch-3_10_0-1062_26_1 (CVE-2021-27364)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>

mail	350459	Средний	Red Hat/CentOS -- уязвимость в kpatch-patch-3_10_0-1062_36_1, kernel, kpatch-patch-3_10_0-1160, kernel-rt, kpatch-patch-3_10_0-957_58_2, kpatch-patch-4_18_0-147_20_1, kpatch-patch-4_18_0-193, kpatch-patch-4_18_0-193_1_2, kpatch-patch-4_18_0-193_13_2, kpatch-patch-4_18_0-193_14_3, kpatch-patch-4_18_0-193_19_1, kpatch-patch-4_18_0-193_28_1, kpatch-patch-4_18_0-193_29_1, kpatch-patch-4_18_0-193_37_1, kpatch-patch-4_18_0-193_40_1, kpatch-patch-4_18_0-193_41_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-4_18_0-193_6_3 (CVE-2021-3347)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7) kernel-tools-libs (0:3.10.0-1062.9.1.el7) python-perf (0:3.10.0-1062.9.1.el7)
mail	355759	Средний	Red Hat/CentOS -- уязвимость в Bind (CVE-2021-25215)
cpe:/o:centos:centos:7			bind-export-libs (32:9.11.4-9.P2.el7) bind-libs-lite (32:9.11.4-9.P2.el7) bind-license (32:9.11.4-9.P2.el7)
mail	357270	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2020-12362)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7) kernel-tools-libs (0:3.10.0-1062.9.1.el7) python-perf (0:3.10.0-1062.9.1.el7)
mail	357334	Средний	Red Hat/CentOS -- уязвимость в Python, python27:2.7, python3, python38:3.8 (CVE-2020-26116)
cpe:/o:centos:centos:7			python (0:2.7.5-86.el7) python-libs (0:2.7.5-86.el7)
mail	357336	Средний	Red Hat/CentOS -- уязвимость в Python, python27:2.7, python-urllib3 (CVE-2020-26137)
cpe:/o:centos:centos:7			python (0:2.7.5-86.el7) python-libs (0:2.7.5-86.el7)
mail	357386	Средний	Red Hat/CentOS -- уязвимость в Python, python27:2.7, python3, python38:3.8 (CVE-2021-3177)
cpe:/o:centos:centos:7			python (0:2.7.5-86.el7) python-libs (0:2.7.5-86.el7)
mail	359154	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-12363)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7) kernel-tools-libs (0:3.10.0-1062.9.1.el7) python-perf (0:3.10.0-1062.9.1.el7)
mail	359155	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-12364)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7) kernel-tools-libs (0:3.10.0-1062.9.1.el7) python-perf (0:3.10.0-1062.9.1.el7)
mail	359157	Средний	Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-24511)
cpe:/o:centos:centos:7			microcode_ctl (2:2.1-53.7.el7_7)
mail	359160	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-27170)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7) kernel (0:3.10.0-514.el7) kernel-tools (0:3.10.0-1062.9.1.el7)

			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	361757	Средний	Red Hat/CentOS -- уязвимость в rpm (CVE-2021-20271)
<i>cpe:/o:centos:centos:7</i>			<i>rpm (0:4.11.3-40.el7)</i>
			<i>rpm-build-libs (0:4.11.3-40.el7)</i>
			<i>rpm-libs (0:4.11.3-40.el7)</i>
			<i>rpm-python (0:4.11.3-40.el7)</i>
mail	364171	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2019-20934)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	364175	Средний	Red Hat/CentOS -- уязвимость в kpatch-patch-3_10_0-1062_36_1, kernel, kernel-rt, kpatch-patch-4_18_0-193_19_1, kpatch-patch-3_10_0-1160, kpatch-patch-3_10_0-957_61_1, kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-305 (CVE-2021-32399)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	365758	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt, kpatch-patch-3_10_0-1062_40_1, kpatch-patch-3_10_0-1160_11_1, kpatch-patch-3_10_0-957_61_1, kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-193_19_1, kpatch-patch-4_18_0-305 (CVE-2021-22543)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	370703	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt, kpatch-patch-3_10_0-1062_43_1, kpatch-patch-3_10_0-1160_11_1, kpatch-patch-3_10_0-957_65_1, kpatch-patch-4_18_0-147_34_1, kpatch-patch-4_18_0-193_37_1, kpatch-patch-4_18_0-305 (CVE-2020-36385)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	371408	Средний	Red Hat/CentOS -- уязвимость в kernel (CVE-2020-27777)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	371448	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2021-29650)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	371460	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2021-3564)

<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-514.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	371461	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2021-3573)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-514.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	372328	Средний	Red Hat/CentOS -- уязвимость в OpenSSL, edk2 (CVE-2021-23840)
<i>cpe:/o:centos:centos:7</i>			<i>openssl (1:1.0.2k-19.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>openssl-libs (1:1.0.2k-19.el7)</i>
mail	372329	Средний	Red Hat/CentOS -- уязвимость в OpenSSL, edk2 (CVE-2021-23841)
<i>cpe:/o:centos:centos:7</i>			<i>openssl (1:1.0.2k-19.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>openssl-libs (1:1.0.2k-19.el7)</i>
mail	372330	Средний	Red Hat/CentOS -- уязвимость в Bind (CVE-2021-25214)
<i>cpe:/o:centos:centos:7</i>			<i>bind-export-libs (32:9.11.4-9.P2.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>bind-libs-lite (32:9.11.4-9.P2.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>bind-license (32:9.11.4-9.P2.el7)</i>
mail	372919	Средний	Red Hat/CentOS -- уязвимость в krb5 (CVE-2021-37750)
<i>cpe:/o:centos:centos:7</i>			<i>krb5-libs (0:1.15.1-37.el7_7.2)</i>
mail	372920	Средний	Red Hat/CentOS -- уязвимость в openssh (CVE-2021-41617)
<i>cpe:/o:centos:centos:7</i>			<i>openssh (0:7.4p1-21.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>openssh-clients (0:7.4p1-21.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>openssh-server (0:7.4p1-21.el7)</i>
mail	378482	Средний	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2016-4658)
<i>cpe:/o:centos:centos:7</i>			<i>libxml2 (0:2.9.1-6.el7_2.3)</i>
mail	378736	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2021-29154)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-514.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	378750	Средний	Red Hat/CentOS -- уязвимость в kpatch-patch-3_10_0-957_84_1, kernel, kernel-rt, kpatch-patch-3_10_0-1160, kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-193_19_1 (CVE-2021-3715)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-514.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	379780	Средний	Red Hat/CentOS -- уязвимость в httpd:2.4, httpd (CVE-2021-34798)
<i>cpe:/o:centos:centos:7</i>			<i>httpd (0:2.4.6-90.el7.centos)</i>
<i>cpe:/o:centos:centos:7</i>			<i>httpd-tools (0:2.4.6-90.el7.centos)</i>
mail	379792	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel, kpatch-patch-4_18_0-147_43_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_46_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_70_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 (CVE-2021-4155)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-514.el7)</i>

kernel-tools (0:3.10.0-1062.9.1.el7)
kernel-tools-libs (0:3.10.0-1062.9.1.el7)
python-perf (0:3.10.0-1062.9.1.el7)

mail	382832	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2020-0465)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	382834	Средний	Red Hat/CentOS -- уязвимость в openldap (CVE-2020-25709)
cpe:/o:centos:centos:7			openldap (0:2.4.44-21.el7_6)
mail	382835	Средний	Red Hat/CentOS -- уязвимость в openldap (CVE-2020-25710)
cpe:/o:centos:centos:7			openldap (0:2.4.44-21.el7_6)
mail	382838	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel, kpatch-patch-4_18_0-147_44_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_49_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_72_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 (CVE-2021-0920)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	382887	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2021-3752)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	382890	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel, kpatch-patch-4_18_0-147_44_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_46_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_72_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 (CVE-2022-0330)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	382893	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel, kpatch-patch-4_18_0-147_44_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_49_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_72_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 (CVE-2022-22942)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	383728	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kernel, kpatch-patch-4_18_0-147_44_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_51_1, kpatch-patch-3_10_0-1160_31_1, kpatch-patch-3_10_0-957_72_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 (CVE-2022-0492)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)

			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	385532	Средний	Red Hat/CentOS -- уязвимость в httpd:2.4, httpd (CVE-2022-22720)
	<i>cpe:/o:centos:centos:7</i>		<i>httpd (0:2.4.6-90.el7.centos)</i>
			<i>httpd-tools (0:2.4.6-90.el7.centos)</i>
mail	390407	Средний	Red Hat/CentOS -- уязвимость в gzip, xz (CVE-2022-1271)
	<i>cpe:/o:centos:centos:7</i>		<i>gzip (0:1.5-10.el7)</i>
mail	394103	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2021-26401)
	<i>cpe:/o:centos:centos:7</i>		<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	403314	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2022-21123)
	<i>cpe:/o:centos:centos:7</i>		<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	403315	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2022-21125)
	<i>cpe:/o:centos:centos:7</i>		<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	403316	Средний	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2022-21166)
	<i>cpe:/o:centos:centos:7</i>		<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	405345	Средний	Red Hat/CentOS -- уязвимость в open-vm-tools (CVE-2022-31676)
	<i>cpe:/o:centos:centos:7</i>		<i>open-vm-tools (0:10.3.0-2.el7_7.1)</i>
			<i>open-vm-tools-desktop (0:10.3.0-2.el7_7.1)</i>
mail	410364	Средний	Red Hat/CentOS -- уязвимость в Bind, bind9.16 (CVE-2022-38177)
	<i>cpe:/o:centos:centos:7</i>		<i>bind-export-libs (32:9.11.4-9.P2.el7)</i>
			<i>bind-libs-lite (32:9.11.4-9.P2.el7)</i>
			<i>bind-license (32:9.11.4-9.P2.el7)</i>
mail	410365	Средний	Red Hat/CentOS -- уязвимость в Bind, bind9.16 (CVE-2022-38178)
	<i>cpe:/o:centos:centos:7</i>		<i>bind-export-libs (32:9.11.4-9.P2.el7)</i>
			<i>bind-libs-lite (32:9.11.4-9.P2.el7)</i>
			<i>bind-license (32:9.11.4-9.P2.el7)</i>
mail	412624	Средний	Red Hat/CentOS -- уязвимость в Bind, bind9.16, DHCP (CVE-2021-25220)
	<i>cpe:/o:centos:centos:7</i>		<i>bind-export-libs (32:9.11.4-9.P2.el7)</i>
			<i>bind-libs-lite (32:9.11.4-9.P2.el7)</i>
			<i>bind-license (32:9.11.4-9.P2.el7)</i>
mail	418857	Средний	Red Hat/CentOS -- уязвимость в kernel-rt, kpatch-patch-5_14_0-70_17_1, kpatch-patch-4_18_0-147_70_1, kernel, kpatch-patch-3_10_0-1160_71_1, kpatch-patch-4_18_0-193_87_1, kpatch-patch-4_18_0-425_3_1, kpatch-patch-5_14_0-162_6_1 (CVE-2022-2964)
	<i>cpe:/o:centos:centos:7</i>		<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>

			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	419822	Средний	Red Hat/CentOS -- уязвимость в Bind (CVE-2022-2795)
<i>cpe:/o:centos:centos:7</i>			<i>bind-export-libs (32:9.11.4-9.P2.el7)</i>
			<i>bind-libs-lite (32:9.11.4-9.P2.el7)</i>
			<i>bind-license (32:9.11.4-9.P2.el7)</i>
mail	288302	Низкий	Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2019-11727)
<i>cpe:/o:centos:centos:7</i>			<i>nspr (0:4.21.0-1.el7)</i>
			<i>nss (0:3.44.0-7.el7_7)</i>
			<i>nss-softokn (0:3.44.0-8.el7_7)</i>
			<i>nss-softokn-freebl (0:3.44.0-8.el7_7)</i>
			<i>nss-sysinit (0:3.44.0-7.el7_7)</i>
			<i>nss-tools (0:3.44.0-7.el7_7)</i>
			<i>nss-util (0:3.44.0-4.el7_7)</i>
mail	307171	Низкий	Red Hat/CentOS -- уязвимость в gettext, emacs-gettext (CVE-2018-18751)
<i>cpe:/o:centos:centos:7</i>			<i>gettext (0:0.19.8.1-2.el7)</i>
			<i>gettext-libs (0:0.19.8.1-2.el7)</i>
mail	307178	Низкий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-10638)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	317784	Низкий	Red Hat/CentOS -- уязвимость в Bind (CVE-2019-6465)
<i>cpe:/o:centos:centos:7</i>			<i>bind-export-libs (32:9.11.4-9.P2.el7)</i>
			<i>bind-libs-lite (32:9.11.4-9.P2.el7)</i>
			<i>bind-license (32:9.11.4-9.P2.el7)</i>
mail	318588	Низкий	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2019-17055)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	320057	Низкий	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2015-8035)
<i>cpe:/o:centos:centos:7</i>			<i>libxml2 (0:2.9.1-6.el7_2.3)</i>
mail	320058	Низкий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2015-9289)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	320065	Низкий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2017-17807)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	320069	Низкий	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2017-18258)
<i>cpe:/o:centos:centos:7</i>			<i>libxml2 (0:2.9.1-6.el7_2.3)</i>

mail	320084	Низкий	Red Hat/CentOS -- уязвимость в polkit (CVE-2018-1116)
cpe:/o:centos:centos:7			polkit (0:0.112-22.el7_7.1)
mail	320090	Низкий	Red Hat/CentOS -- уязвимость в httpd (CVE-2018-1301)
cpe:/o:centos:centos:7			httpd (0:2.4.6-90.el7.centos)
			httpd-tools (0:2.4.6-90.el7.centos)
mail	320132	Низкий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-10639)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	320134	Низкий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-11190)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	323684	Низкий	Red Hat/CentOS -- уязвимость в libtiff (CVE-2019-14973)
cpe:/o:centos:centos:7			libtiff (0:4.0.3-32.el7)
mail	323687	Низкий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-17053)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)
			kernel-tools-libs (0:3.10.0-1062.9.1.el7)
			python-perf (0:3.10.0-1062.9.1.el7)
mail	324127	Низкий	Red Hat/CentOS -- уязвимость в libmspack (CVE-2019-1010305)
cpe:/o:centos:centos:7			libmspack (0:0.5-0.7.alpha.el7)
mail	324147	Низкий	Red Hat/CentOS -- уязвимость в dnsmasq (CVE-2019-14834)
cpe:/o:centos:centos:7			dnsmasq (0:2.76-10.el7_7.1)
mail	324161	Низкий	Red Hat/CentOS -- уязвимость в glibc (CVE-2019-19126)
cpe:/o:centos:centos:7			glibc (0:2.17-292.el7)
			glibc-common (0:2.17-292.el7)
mail	324173	Низкий	Red Hat/CentOS -- уязвимость в cups (CVE-2019-8675)
cpe:/o:centos:centos:7			cups-libs (1:1.6.3-40.el7)
mail	324174	Низкий	Red Hat/CentOS -- уязвимость в cups (CVE-2019-8696)
cpe:/o:centos:centos:7			cups-libs (1:1.6.3-40.el7)
mail	326424	Низкий	Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-0548)
cpe:/o:centos:centos:7			microcode_ctl (2:2.1-53.7.el7_7)
mail	333906	Низкий	Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2020-12402)
cpe:/o:centos:centos:7			nspr (0:4.21.0-1.el7)
			nss (0:3.44.0-7.el7_7)
			nss-softokn (0:3.44.0-8.el7_7)
			nss-softokn-freebl (0:3.44.0-8.el7_7)
			nss-sysinit (0:3.44.0-7.el7_7)
			nss-tools (0:3.44.0-7.el7_7)
			nss-util (0:3.44.0-4.el7_7)
mail	337341	Низкий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-16231)
cpe:/o:centos:centos:7			kernel (0:3.10.0-1062.9.1.el7)
			kernel (0:3.10.0-514.el7)
			kernel-tools (0:3.10.0-1062.9.1.el7)

			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337342	Низкий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-16233)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337356	Низкий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19537)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337364	Низкий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10732)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337756	Низкий	Red Hat/CentOS -- уязвимость в httpd (CVE-2017-15715)
<i>cpe:/o:centos:centos:7</i>			<i>httpd (0:2.4.6-90.el7.centos)</i>
			<i>httpd-tools (0:2.4.6-90.el7.centos)</i>
mail	337769	Низкий	Red Hat/CentOS -- уязвимость в httpd:2.4 (CVE-2019-10098)
<i>cpe:/o:centos:centos:7</i>			<i>httpd (0:2.4.6-90.el7.centos)</i>
			<i>httpd-tools (0:2.4.6-90.el7.centos)</i>
mail	337774	Низкий	Red Hat/CentOS -- уязвимость в kernel (CVE-2019-12614)
<i>cpe:/o:centos:centos:7</i>			<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	337788	Низкий	Red Hat/CentOS -- уязвимость в systemd (CVE-2019-20386)
<i>cpe:/o:centos:centos:7</i>			<i>libgudev1 (0:219-67.el7_7.2)</i>
			<i>systemd (0:219-67.el7_7.2)</i>
			<i>systemd-libs (0:219-67.el7_7.2)</i>
			<i>systemd-sysv (0:219-67.el7_7.2)</i>
mail	337903	Низкий	Red Hat/CentOS -- уязвимость в NetworkManager (CVE-2020-10754)
<i>cpe:/o:centos:centos:7</i>			<i>NetworkManager (1:1.18.0-5.el7_7.1)</i>
			<i>NetworkManager-libnm (1:1.18.0-5.el7_7.1)</i>
			<i>NetworkManager-ppp (1:1.18.0-5.el7_7.1)</i>
			<i>NetworkManager-team (1:1.18.0-5.el7_7.1)</i>
			<i>NetworkManager-tui (1:1.18.0-5.el7_7.1)</i>
			<i>NetworkManager-wifi (1:1.18.0-5.el7_7.1)</i>
mail	337912	Низкий	Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2020-12400)
<i>cpe:/o:centos:centos:7</i>			<i>nspr (0:4.21.0-1.el7)</i>
			<i>nss (0:3.44.0-7.el7_7)</i>
			<i>nss-softokn (0:3.44.0-8.el7_7)</i>
			<i>nss-softokn-freebl (0:3.44.0-8.el7_7)</i>
			<i>nss-sysinit (0:3.44.0-7.el7_7)</i>
			<i>nss-tools (0:3.44.0-7.el7_7)</i>

			<i>nss-util (0:3.44.0-4.el7_7)</i>
mail	337913	Низкий	Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2020-12401)
	<i>cpe:/o:centos:centos:7</i>		<i>nspr (0:4.21.0-1.el7)</i>
			<i>nss (0:3.44.0-7.el7_7)</i>
			<i>nss-softokn (0:3.44.0-8.el7_7)</i>
			<i>nss-softokn-freebl (0:3.44.0-8.el7_7)</i>
			<i>nss-sysinit (0:3.44.0-7.el7_7)</i>
			<i>nss-tools (0:3.44.0-7.el7_7)</i>
			<i>nss-util (0:3.44.0-4.el7_7)</i>
mail	337932	Низкий	Red Hat/CentOS -- уязвимость в httpd:2.4 (CVE-2020-1934)
	<i>cpe:/o:centos:centos:7</i>		<i>httpd (0:2.4.6-90.el7.centos)</i>
			<i>httpd-tools (0:2.4.6-90.el7.centos)</i>
mail	337978	Низкий	Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2020-6829)
	<i>cpe:/o:centos:centos:7</i>		<i>nspr (0:4.21.0-1.el7)</i>
			<i>nss (0:3.44.0-7.el7_7)</i>
			<i>nss-softokn (0:3.44.0-8.el7_7)</i>
			<i>nss-softokn-freebl (0:3.44.0-8.el7_7)</i>
			<i>nss-sysinit (0:3.44.0-7.el7_7)</i>
			<i>nss-tools (0:3.44.0-7.el7_7)</i>
			<i>nss-util (0:3.44.0-4.el7_7)</i>
mail	341337	Низкий	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2019-20811)
	<i>cpe:/o:centos:centos:7</i>		<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	341422	Низкий	Red Hat/CentOS -- уязвимость в Bind (CVE-2020-8624)
	<i>cpe:/o:centos:centos:7</i>		<i>bind-export-libs (32:9.11.4-9.P2.el7)</i>
			<i>bind-libs-lite (32:9.11.4-9.P2.el7)</i>
			<i>bind-license (32:9.11.4-9.P2.el7)</i>
mail	341425	Низкий	Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-8696)
	<i>cpe:/o:centos:centos:7</i>		<i>microcode_ctl (2:2.1-53.7.el7_7)</i>
mail	345785	Низкий	Red Hat/CentOS -- уязвимость в dnsmasq (CVE-2020-25684)
	<i>cpe:/o:centos:centos:7</i>		<i>dnsmasq (0:2.76-10.el7_7.1)</i>
mail	345786	Низкий	Red Hat/CentOS -- уязвимость в dnsmasq (CVE-2020-25685)
	<i>cpe:/o:centos:centos:7</i>		<i>dnsmasq (0:2.76-10.el7_7.1)</i>
mail	345787	Низкий	Red Hat/CentOS -- уязвимость в dnsmasq (CVE-2020-25686)
	<i>cpe:/o:centos:centos:7</i>		<i>dnsmasq (0:2.76-10.el7_7.1)</i>
mail	350028	Низкий	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-25656)
	<i>cpe:/o:centos:centos:7</i>		<i>kernel (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel (0:3.10.0-514.el7)</i>
			<i>kernel-tools (0:3.10.0-1062.9.1.el7)</i>
			<i>kernel-tools-libs (0:3.10.0-1062.9.1.el7)</i>
			<i>python-perf (0:3.10.0-1062.9.1.el7)</i>
mail	357235	Низкий	Red Hat/CentOS -- уязвимость в libpng (CVE-2017-12652)
	<i>cpe:/o:centos:centos:7</i>		<i>libpng (2:1.5.13-7.el7_2)</i>
mail	359158	Низкий	Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-24512)
	<i>cpe:/o:centos:centos:7</i>		<i>microcode_ctl (2:2.1-53.7.el7_7)</i>

Список уязвимостей

Уязвимость	Риск: Критический
ALTX ID 317797	Red Hat/CentOS -- уязвимость в rpp (CVE-2020-8597)
Описание	
В продукте rpp обнаружена уязвимость CVE-2020-8597.	
Исправление	
Необходимо установить актуальное обновление от производителя.	
Ссылки	
oval:ru.altx-soft.nix:def:127683 https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:127683	
VULN-20221109.4 (NKCKI) https://safe-surf.ru/upload/VULN/VULN-20221109.4.pdf	
VULN-20221109.2 (NKCKI) https://safe-surf.ru/upload/VULN/VULN-20221109.2.pdf	
CESA-2020:0631 (CESA-2020:0631) http://lists.centos.org/pipermail/centos-announce/2020-February/035650.html	
CESA-2020:0630 (CESA-2020:0630) http://lists.centos.org/pipermail/centos-announce/2020-February/035652.html	
VULN-20200818.4 (NKCKI) http://safe-surf.ru/upload/VULN/VULN-20200818.4.pdf	
BDU:2020-01026 (FSTEC) https://bdu.fstec.ru/vul/2020-01026	
CVE-2020-8597 (CVE) CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P) CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) CWE-120 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8597	
RHSA-2020:0633 (VENDOR) https://access.redhat.com/errata/RHSA-2020:0633	
RHSA-2020:0631 (VENDOR) https://access.redhat.com/errata/RHSA-2020:0631	
RHSA-2020:0630 (VENDOR) https://access.redhat.com/errata/RHSA-2020:0630	

Уязвимость	Риск: Критический
ALTX ID 358388	Red Hat/CentOS -- уязвимость в glib2 (CVE-2021-27219)
Описание	
В продукте glib2 обнаружена уязвимость CVE-2021-27219.	
Исправление	
Необходимо установить актуальное обновление от производителя.	
Ссылки	
oval:ru.altx-soft.nix:def:154557 https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:154557	

VULN-20220110.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220110.2.pdf>

CESA-2021:2147 (CESA-2021:2147)

<http://lists.centos.org/pipermail/centos-announce/2021-June/048328.html>

RHSA-2021:2467 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2467>

BDU:2021-00680 (FSTEC)

<https://bdu.fstec.ru/vul/2021-00680>

CVE-2021-27219 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-681

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27219>

RHSA-2021:2147 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2147>

RHSA-2021:2170 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2170>

RHSA-2021:2171 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2171>

RHSA-2021:2172 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2172>

RHSA-2021:2203 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2203>

RHSA-2021:2175 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2175>

RHSA-2021:2174 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2174>

RHSA-2021:2173 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2173>

RHSA-2021:2204 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2204>

Уязвимость	Риск: Критический
ALTX ID 372948	Red Hat/CentOS -- уязвимость в nss, thunderbird (CVE-2021-43527)
Описание	

В продуктах nss, thunderbird обнаружена уязвимость CVE-2021-43527.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:164628

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:164628>

RHSA-2021:4969 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4969>

VULN-20220601.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220601.2.pdf>

VULN-20220516.3 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220516.3.pdf>

VULN-20220124.8 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220124.8.pdf>

BDU:2022-00002 (FSTEC)

<https://bdu.fstec.ru/vul/2022-00002>

CESA-2021:4904 (CESA-2021:4904)

<http://lists.centos.org/pipermail/centos-announce/2021-December/060972.html>

VULN-20211206.9 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20211206.9.pdf>

RHSA-2021:4954 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4954>

RHSA-2021:4953 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4953>

RHSA-2021:4946 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4946>

RHSA-2021:4933 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4933>

RHSA-2021:4932 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4932>

RHSA-2021:4994 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4994>

CVE-2021-43527 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43527>

RHSA-2021:4907 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4907>

RHSA-2021:4904 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4904>

RHSA-2021:4903 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4903>

RHSA-2021:4909 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4909>

RHSA-2021:4919 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4919>

Уязвимость	Риск: Критический
ALTX ID 383732	Red Hat/CentOS -- уязвимость в firefox, thunderbird, expat (CVE-2022-25236)
Описание	

В продуктах firefox, thunderbird, expat обнаружена уязвимость CVE-2022-25236.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:172037

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:172037>

RHSA-2022:0815 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0815>

RHSA-2022:0847 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0847>

RHSA-2022:1068 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1068>

VULN-20221005.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

RHSA-2022:1309 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1309>

CESA-2022:0824 (CESA-2022:0824)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073578.html>

CESA-2022:0850 (CESA-2022:0850)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073579.html>

RHSA-2022:1069 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1069>

CESA-2022:1069 (CESA-2022:1069)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073580.html>

RHSA-2022:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1070>

RHSA-2022:1012 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1012>

RHSA-2022:0843 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0843>

RHSA-2022:0853 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0853>

RHSA-2022:0850 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0850>

RHSA-2022:0845 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0845>

RHSA-2022:0951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0951>

BDU:2022-01065 (FSTEC)

<https://bdu.fstec.ru/vul/2022-01065>

CVE-2022-25236 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-668

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25236>

RHSA-2022:0817 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0817>

RHSA-2022:0816 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0816>

RHSA-2022:0818 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0818>

RHSA-2022:0824 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0824>

Уязвимость	Риск: Высокий
ALTX ID 205829	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2016-5131)
Описание	В продукте libxml2 обнаружена уязвимость CVE-2016-5131.
Исправление	Необходимо установить актуальное обновление от производителя.
Ссылки	

oval:ru.altx-soft.nix:def:35671

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:35671>

CESA-2020:1190 (CESA-2020:1190)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012518.html>

RHSA-2020:1190 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1190>

CVE-2016-5131 (CVE)

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5131>

RHSA-2016:1485 (VENDOR)

<https://rhn.redhat.com/errata/RHSA-2016-1485.html>

Уязвимость

Риск: Высокий

ALTX ID

207017

Red Hat/CentOS -- уязвимость в libxml2 (CVE-2017-15412)

Описание

В продукте libxml2 обнаружена уязвимость CVE-2017-15412.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:36859

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:36859>

CESA-2020:1190 (CESA-2020:1190)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012518.html>

RHSA-2020:1190 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1190>

CVE-2017-15412 (CVE)

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15412>

RHSA-2017:3401 (VENDOR)

<https://access.redhat.com/errata/RHSA-2017:3401>

Уязвимость

Риск: Высокий

ALTX ID

211012

Red Hat -- уязвимость в expat (CVE-2015-2716)

Описание

В продукте expat обнаружена уязвимость CVE-2015-2716.

Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта [a href="https://www.mozilla.org/ru/firefox/new/">https://www.mozilla.org/ru/firefox/new/](https://www.mozilla.org/ru/firefox/new/), <https://www.mozilla.org/ru/thunderbird/>.

Ссылки

oval:ru.altx-soft.nix:def:40854

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:40854>

BDU:2021-03335 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03335>

CESA-2020:1011 (CESA-2020:1011)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012444.html>

RHSA-2020:2508 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2508>

RHSA-2020:1011 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1011>

CVE-2015-2716 (CVE)

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CWE-119

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2716>

RHSA-2015:0988 (VENDOR)

<https://rhn.redhat.com/errata/RHSA-2015-0988.html>

CESA-2015:0988-CentOS 6 (CESA-2015:0988)

<http://lists.centos.org/pipermail/centos-announce/2015-May/021104.html>

CESA-2015:0988-CentOS 7 (CESA-2015:0988)

<http://lists.centos.org/pipermail/centos-announce/2015-May/021132.html>

CESA-2015:0988-CentOS 5 (CESA-2015:0988)

<http://lists.centos.org/pipermail/centos-announce/2015-May/021133.html>

RHSA-2015:1012 (VENDOR)

<https://rhn.redhat.com/errata/RHSA-2015-1012.html>

CESA-2015:1012-CentOS 7 (CESA-2015:1012)

<http://lists.centos.org/pipermail/centos-announce/2015-May/021143.html>

CESA-2015:1012-CentOS 6 (CESA-2015:1012)

<http://lists.centos.org/pipermail/centos-announce/2015-May/021144.html>

CESA-2015:1012-CentOS 5 (CESA-2015:1012)

<http://lists.centos.org/pipermail/centos-announce/2015-May/021145.html>

Уязвимость

Риск: Высокий

ALTX ID

291909

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-11487)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-11487.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:106802

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:106802>

CESA-2020:0839 (CESA-2020:0839)

<http://lists.centos.org/pipermail/centos-announce/2020-March/035660.html>

CESA-2020:4182 (CESA-2020:4182)

<http://lists.centos.org/pipermail/centos-announce/2020-November/035811.html>

RHSA-2020:4182 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4182>

RHSA-2020:2851 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2851>

RHSA-2020:3230 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3230>

RHSA-2020:0834 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0834>

RHSA-2020:0839 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0839>

RHSA-2019:2703 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:2703>

BDU:2019-02763 (FSTEC)

<https://bdu.fstec.ru/vul/2019-02763>

CVE-2019-11487 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.8 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11487>

RHSA-2019:2741 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:2741>

Уязвимость	Риск: Высокий
ALTX ID 295855	Red Hat/CentOS -- уязвимость в thunderbird, expat (CVE-2019-15903)
Описание	

В продуктах thunderbird, expat обнаружена уязвимость CVE-2019-15903.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:109850

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:109850>

CESA-2020:3952 (CESA-2020:3952)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012694.html>

RHSA-2020:4484 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4484>

RHSA-2020:3952 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3952>

CESA-2019:3756 (CESA-2019:3756)

<http://lists.centos.org/pipermail/centos-announce/2019-November/023514.html>

RHSA-2019:3756 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3756>

BDU:2019-03643 (FSTEC)

<https://bdu.fstec.ru/vul/2019-03643>

CVE-2019-15903 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 5.5 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15903>

RHSA-2019:3237 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3237>

RHSA-2019:3210 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3210>

CESA-2019:3210 (CESA-2019:3210)

<http://lists.centos.org/pipermail/centos-announce/2019-October/023498.html>

Уязвимость

Риск: Высокий

ALTX ID
311018**Red Hat/CentOS -- уязвимость в chromium-browser, sqlite (CVE-2019-13734)****Описание**

В продуктах chromium-browser, sqlite обнаружена уязвимость CVE-2019-13734.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:123002**<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:123002>**CESA-2020:0227 (CESA-2020:0227)**<http://lists.centos.org/pipermail/centos-announce/2020-January/035616.html>**RHSA-2020:2014 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:2014>**VULN-20200506.8 (NKCKI)**<http://safe-surf.ru/upload/VULN/VULN-20200506.8.pdf>**BDU:2020-01700 (FSTEC)**<https://bdu.fstec.ru/vul/2020-01700>**VULN-20191224.3 (NKCKI)**<http://safe-surf.ru/upload/VULN/VULN-20191224.3.pdf>**RHSA-2020:0227 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:0227>**RHSA-2020:0273 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:0273>**CVE-2019-13734 (CVE)**

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13734>**RHSA-2019:4238 (VENDOR)**<https://access.redhat.com/errata/RHSA-2019:4238>**Уязвимость**

Риск: Высокий

ALTX ID
316323**Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-14816)****Описание**

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-14816.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:126762**<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:126762>**CESA-2020:0375 (CESA-2020:0375)**<http://lists.centos.org/pipermail/centos-announce/2020-February/035620.html>

CESA-2020:0374 (CESA-2020:0374)

<http://lists.centos.org/pipermail/centos-announce/2020-February/035645.html>

RHSA-2020:0664 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0664>

RHSA-2020:0661 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0661>

RHSA-2020:0653 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0653>

RHSA-2020:1266 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1266>

RHSA-2020:1347 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1347>

BDU-2020-03327 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03327>

RHSA-2020:0374 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0374>

CVE-2019-14816 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 8.0 (CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-122

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14816>

RHSA-2020:0375 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0375>

RHSA-2020:0339 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0339>

RHSA-2020:0328 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0328>

Уязвимость	Риск: Высокий
ALTX ID	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-14895)
316325	

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-14895.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:126764

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:126764>

CESA-2020:0375 (CESA-2020:0375)

<http://lists.centos.org/pipermail/centos-announce/2020-February/035620.html>

CESA-2020:0374 (CESA-2020:0374)

<http://lists.centos.org/pipermail/centos-announce/2020-February/035645.html>

RHSA-2020:0543 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0543>

RHSA-2020:0592 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0592>

RHSA-2020:0664 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0664>

RHSA-2020:0661 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0661>

RHSA-2020:0653 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0653>

RHSA-2020:0374 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0374>

BDU:2019-04799 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04799>

CVE-2019-14895 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.0 (CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-122

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14895>

RHSA-2020:0375 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0375>

RHSA-2020:0339 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0339>

RHSA-2020:0328 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0328>

Уязвимость	Риск: Высокий
ALTX ID 316327	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-14901)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-14901.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:126766

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:126766>

CESA-2020:0375 (CESA-2020:0375)

<http://lists.centos.org/pipermail/centos-announce/2020-February/035620.html>

CESA-2020:0374 (CESA-2020:0374)

<http://lists.centos.org/pipermail/centos-announce/2020-February/035645.html>

RHSA-2020:0374 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0374>

BDU:2019-04788 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04788>

CVE-2019-14901 (CVE)

CVSSv2: Базовая оценка 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 8.8 (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-400

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14901>

RHSA-2020:0375 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0375>

RHSA-2020:0339 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0339>

RHSA-2020:0328 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0328>

Уязвимость	Риск: Высокий
-------------------	---------------

ALTX ID

316329

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-17133)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-17133.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:126768

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:126768>

CESA-2020:0375 (CESA-2020:0375)

<http://lists.centos.org/pipermail/centos-announce/2020-February/035620.html>

CESA-2020:0374 (CESA-2020:0374)

<http://lists.centos.org/pipermail/centos-announce/2020-February/035645.html>

CESA-2020:0790 (CESA-2020:0790)

<http://lists.centos.org/pipermail/centos-announce/2020-March/035659.html>

RHSA-2020:0543 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0543>

RHSA-2020:0592 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0592>

RHSA-2020:0664 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0664>

RHSA-2020:0661 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0661>

RHSA-2020:0653 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0653>

RHSA-2020:0790 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0790>

RHSA-2020:0374 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0374>

BDU:2020-00078 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00078>

CVE-2019-17133 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.0 (CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CWE-120

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17133>

RHSA-2020:0375 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0375>

Уязвимость

Риск: Высокий

ALTX ID

316895

Red Hat/CentOS -- уязвимость в sudo (CVE-2019-18634)

Описание

В продукте sudo обнаружена уязвимость CVE-2019-18634.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:126912

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:126912>

CESA-2020:0540 (CESA-2020:0540)

<http://lists.centos.org/pipermail/centos-announce/2020-February/035643.html>

CESA-2020:0726 (CESA-2020:0726)

<http://lists.centos.org/pipermail/centos-announce/2020-March/035656.html>

RHSA-2020:0726 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0726>

BDU:2020-00855 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00855>

RHSA-2020:0540 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0540>

CVE-2019-18634 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18634>

RHSA-2020:0487 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0487>

Уязвимость	Риск: Высокий
ALTX ID 317766	Red Hat/CentOS -- уязвимость в evolution-data-server, evolution, evolution-ews, atk (CVE-2019-3890)
Описание	

В продукте evolution-data-server, evolution, evolution-ews, atk обнаружена уязвимость CVE-2019-3890.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:127652

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:127652>

CESA-2020:1080-CentOS 7 (CESA-2020:1080)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012408.html>

RHSA-2020:1080 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1080>

CVE-2019-3890 (CVE)

CVSSv2: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSSv3: Базовая оценка 8.1 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N)

CWE-295

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-3890>

RHSA-2019:3699 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3699>

Уязвимость	Риск: Высокий
ALTX ID 319001	Red Hat/CentOS -- уязвимость в icu, nodejs (CVE-2020-10531)
Описание	

В продуктах icu, nodejs обнаружена уязвимость CVE-2020-10531.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:128435

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:128435>

CESA-2020:0897 (CESA-2020:0897)

<http://lists.centos.org/pipermail/centos-announce/2020-March/035682.html>

CESA-2020:0896 (CESA-2020:0896)

<http://lists.centos.org/pipermail/centos-announce/2020-March/035688.html>

BDU:2020-02034 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02034>

VULN-20200415.1 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20200415.1.pdf>

RHSA-2020:1317 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1317>

VULN-20200319.2 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20200319.2.pdf>

RHSA-2020:1293 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1293>

CVE-2020-10531 (CVE)

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10531>

RHSA-2020:0902 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0902>

RHSA-2020:0897 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0897>

RHSA-2020:0896 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0896>

Уязвимость

Риск: Высокий

ALTX ID

320180

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-16746)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-16746.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129228

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129228>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

BDU:2019-03507 (FSTEC)

<https://bdu.fstec.ru/vul/2019-03507>

CVE-2019-16746 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.3 (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-120

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16746>

RHSA-2020:1070 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:1070>**RHSA-2020:1016 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1016>**Уязвимость**

Риск: Высокий

ALT X ID

325927

Red Hat/CentOS -- уязвимость в Bind, bind-chroot, bind-devel, bind-libs, bind-libs-lite, bind-license, bind-lite-devel, bind-pkcs11, bind-pkcs11-devel, bind-pkcs11-libs, bind-pkcs11-utils, bind-sdb, bind-sdb-chroot, bind-utils, bind-debugsource, bind-export-devel, bind-export-libs, python3-bind (CVE-2020-8616)**Описание**

В продукте Bind, bind-chroot, bind-devel, bind-libs, bind-libs-lite, bind-license, bind-lite-devel, bind-pkcs11, bind-pkcs11-devel, bind-pkcs11-libs, bind-pkcs11-utils, bind-sdb, bind-sdb-chroot, bind-utils, bind-debugsource, bind-export-devel, bind-export-libs, python3-bind обнаружена уязвимость CVE-2020-8616.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:132352**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:132352>**RHSA-2020:2338 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:2338>**CESA-2020:2383 (CESA-2020:2383)**<http://lists.centos.org/pipermail/centos-announce/2020-June/035748.html>**BDU:2020-03950 (FSTEC)**<https://bdu.fstec.ru/vuln/2020-03950>**RHSA-2020:3475 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3475>**RHSA-2020:3471 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3471>**RHSA-2020:3470 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3470>**RHSA-2020:3433 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3433>**RHSA-2020:3379 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3379>**RHSA-2020:3378 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3378>**RHSA-2020:3272 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3272>**VULN-20200522.3 (NKCKI)**<http://safe-surf.ru/upload/VULN/VULN-20200522.3.pdf>**CVE-2020-8616 (CVE)**

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)

CWE-400

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8616>**RHSA-2020:2345 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:2345>**RHSA-2020:2344 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:2344>**CESA-2020:2344 (CESA-2020:2344)**<http://lists.centos.org/pipermail/centos-announce/2020-June/035744.html>

RHSA-2020:2383 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2383>

Уязвимость

Риск: Высокий

ALT X ID
325928

Red Hat/CentOS -- уязвимость в Bind, bind-chroot, bind-devel, bind-libs, bind-libs-lite, bind-license, bind-lite-devel, bind-pkcs11, bind-pkcs11-devel, bind-pkcs11-libs, bind-pkcs11-utils, bind-sdb, bind-sdb-chroot, bind-utils, bind-debugsource, bind-export-devel, bind-export-libs, python3-bind (CVE-2020-8617)

Описание

В продукте Bind, bind-chroot, bind-devel, bind-libs, bind-libs-lite, bind-license, bind-lite-devel, bind-pkcs11, bind-pkcs11-devel, bind-pkcs11-libs, bind-pkcs11-utils, bind-sdb, bind-sdb-chroot, bind-utils, bind-debugsource, bind-export-devel, bind-export-libs, python3-bind обнаружена уязвимость CVE-2020-8617.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:132353

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:132353>

RHSA-2020:2338 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2338>

CESA-2020:2383 (CESA-2020:2383)

<http://lists.centos.org/pipermail/centos-announce/2020-June/035748.html>

RHSA-2020:2893 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2893>

BDU:2021-00125 (FSTEC)

<https://bdu.fstec.ru/vul/2021-00125>

RHSA-2020:3475 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3475>

RHSA-2020:3471 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3471>

RHSA-2020:3470 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3470>

RHSA-2020:3433 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3433>

RHSA-2020:3379 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3379>

RHSA-2020:3378 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3378>

VULN-20200522.3 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20200522.3.pdf>

CVE-2020-8617 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-617

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8617>

RHSA-2020:2345 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2345>

RHSA-2020:2344 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2344>

CESA-2020:2344 (CESA-2020:2344)

<http://lists.centos.org/pipermail/centos-announce/2020-June/035744.html>

RHSA-2020:2383 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2383>

Уязвимость

Риск: Высокий

ALTX ID
330683**Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19807)****Описание**

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19807.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:135392**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:135392>**CESA-2020:4060 (CESA-2020:4060)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>**RHSA-2020:4060 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4060>**RHSA-2020:4062 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4062>**RHSA-2020:3222 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3222>**RHSA-2020:3010 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3010>**BDU:2020-00854 (FSTEC)**<https://bdu.fstec.ru/vul/2020-00854>**CVE-2019-19807 (CVE)**

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19807>**RHSA-2020:3016 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3016>**Уязвимость**

Риск: Высокий

ALTX ID
332426**Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-10713)****Описание**

В продуктах grub2, shim, fwupd обнаружена уязвимость CVE-2020-10713.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:137027**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:137027>**RHSA-2020:3227 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3227>**CESA-2020:3217-CentOS 7 (CESA-2020:3217)**<http://lists.centos.org/pipermail/centos-announce/2020-July/035781.html>**RHSA-2020:3274 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3274>

RHSA-2020:3275 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3275>

VULN-20200813.8 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20200813.8.pdf>

RHSA-2020:3271 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3271>

RHSA-2020:3273 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3273>

RHSA-2020:3276 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3276>

BDU:2020-03625 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03625>

CVE-2020-10713 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.1 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)

CWE-120

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10713>

RHSA-2020:3216 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3216>

RHSA-2020:3217 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3217>

RHSA-2020:3223 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3223>

Уязвимость	Риск: Высокий
ALTX ID 333903	Red Hat/CentOS -- уязвимость в nspr, nss, nss-softokn (CVE-2019-17006)
Описание	

В продуктах nspr, nss, nss-softokn обнаружена уязвимость CVE-2019-17006.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:138453

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:138453>

CESA-2020:4076-CentOS 7 (CESA-2020:4076)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-November/012876.html>

RHSA-2021:1026 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1026>

RHSA-2021:0876 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0876>

RHSA-2021:0758 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0758>

RHSA-2020:4076 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4076>

BDU:2020-02871 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02871>

CVE-2019-17006 (CVE)

CVSSv2: Базовая оценка 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-119

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17006>

RHSA-2020:3280 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:3280>

Уязвимость	Риск: Высокий
ALT X ID 337352	Red Hat/CentOS -- уязвимость в kernel (CVE-2019-19447)
Описание	

В продукте kernel обнаружена уязвимость CVE-2019-19447.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:140484**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140484>**RHSA-2020:5656 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5656>**RHSA-2020:5430 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5430>**RHSA-2020:5206 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5206>**RHSA-2020:4609 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4609>**RHSA-2020:4431 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4431>**CESA-2020:4060 (CESA-2020:4060)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>**RHSA-2020:4060 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4060>**BDU:2020-00305 (FSTEC)**<https://bdu.fstec.ru/vul/2020-00305>**CVE-2019-19447 (CVE)**

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.8 (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19447>**RHSA-2020:4062 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость	Риск: Высокий
ALT X ID 337397	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-14305)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-14305.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:140529**

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140529>

BDU:2021-00130 (FSTEC)

<https://bdu.fstec.ru/vul/2021-00130>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2020-14305 (CVE)

CVSSv2: Базовая оценка 8.3 (AV:N/AC:M/Au:N/C:P/I:P/A:C)

CVSSv3: Базовая оценка 8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14305>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Высокий

ALTX ID

337768

Red Hat/CentOS -- уязвимость в expat (CVE-2018-20843)

Описание

В продукте expat обнаружена уязвимость CVE-2018-20843.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140835

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140835>

BDU:2019-03327 (FSTEC)

<https://bdu.fstec.ru/vul/2019-03327>

RHSA-2020:4484 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4484>

CESA-2020:3952 (CESA-2020:3952)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012694.html>

CVE-2018-20843 (CVE)

CVSSv2: Базовая оценка 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

CWE-611

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20843>

RHSA-2020:3952 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3952>

Уязвимость

Риск: Высокий

ALTX ID

337784

Red Hat/CentOS -- уязвимость в libtiff (CVE-2019-17546)

Описание

В продукте libtiff обнаружена уязвимость CVE-2019-17546.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140851

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140851>

VULN-20221005.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

BDU:2021-03591 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03591>

RHSA-2020:4634 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4634>

CESA-2020:3902 (CESA-2020:3902)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012763.html>

CVE-2019-17546 (CVE)

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17546>

RHSA-2020:3902 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3902>

Уязвимость

Риск: Высокий

ALTX ID

337794

Red Hat/CentOS -- уязвимость в e2fsprogs (CVE-2019-5188)

Описание

В продукте e2fsprogs обнаружена уязвимость CVE-2019-5188.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140861

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140861>

VULN-20220727.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.2.pdf>

BDU:2021-03599 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03599>

CESA-2020:4011 (CESA-2020:4011)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012685.html>

CVE-2019-5188 (CVE)

CVSSv2: Базовая оценка 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5188>

RHSA-2020:4011 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4011>

Уязвимость

Риск: Высокий

ALTX ID

340349

Red Hat/CentOS -- уязвимость в chromium-browser, freetype (CVE-2020-15999)

Описание

В продуктах chromium-browser, freetype обнаружена уязвимость CVE-2020-15999.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:142356

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:142356>

VULN-20201027.4 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20201027.4.pdf>

BDU:2020-05385 (FSTEC)

<https://bdu.fstec.ru/vul/2020-05385>

VULN-20201125.12 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20201125.12.pdf>

RHSA-2020:4907 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4907>

CESA-2020:4907 (CESA-2020:4907)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-November/012870.html>

RHSA-2020:4951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4951>

RHSA-2020:4952 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4952>

RHSA-2020:4950 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4950>

CVE-2020-15999 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15999>

RHSA-2020:4351 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4351>

Уязвимость

Риск: Высокий

ALTX ID

341389

Red Hat/CentOS -- уязвимость в libx11, mesa, libdrm, libwacom, xorg-x11-drivers, egl-wayland, libglvnd, libinput (CVE-2020-14363)

Описание

В продукте libx11, mesa, libdrm, libwacom, xorg-x11-drivers, egl-wayland, libglvnd, libinput обнаружена уязвимость CVE-2020-14363.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:143077

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:143077>

RHSA-2021:1804 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1804>

BDU:2021-02599 (FSTEC)

<https://bdu.fstec.ru/vul/2021-02599>

CVE-2020-14363 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14363>

RHSA-2020:4908 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4908>

CESA-2020:4908 (CESA-2020:4908)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-November/012875.html>

RHSA-2020:4946 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4946>

CESA-2020:4946 (CESA-2020:4946)

<http://lists.centos.org/pipermail/centos-announce/2020-November/035816.html>

Уязвимость	Риск: Высокий
ALT X ID 343988	Red Hat/CentOS -- уязвимость в linux-firmware, iwl1000-firmware, iwl100-firmware, iwl105-firmware, iwl135-firmware, iwl2000-firmware, iwl2030-firmware, iwl3160-firmware, iwl3945-firmware, iwl4965-firmware, iwl5000-firmware, iwl5150-firmware, iwl6000-firmware, iwl6000g2a-firmware, iwl6000g2b-firmware, iwl6050-firmware, iwl7260-firmware, libertas-sd8686-firmware, libertas-sd8787-firmware, libertas-usb8388-firmware, libertas-usb8388-olpc-firmware (CVE-2020-12321)

Описание

В продукте linux-firmware, iwl1000-firmware, iwl100-firmware, iwl105-firmware, iwl135-firmware, iwl2000-firmware, iwl2030-firmware, iwl3160-firmware, iwl3945-firmware, iwl4965-firmware, iwl5000-firmware, iwl5150-firmware, iwl6000-firmware, iwl6000g2a-firmware, iwl6000g2b-firmware, iwl6050-firmware, iwl7260-firmware, libertas-sd8686-firmware, libertas-sd8787-firmware, libertas-usb8388-firmware, libertas-usb8388-olpc-firmware обнаружена уязвимость CVE-2020-12321.

Исправление

Необходимо установить актуальное обновление от производителя.

- Ссылки**
- oval:ru.altx-soft.nix:def:145160
<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:145160>
 - RHSA-2022:7887 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:7887>
 - VULN-20221021.3 (NKCKI)**
<https://safe-surf.ru/upload/VULN/VULN-20221021.3.pdf>
 - CESA-2021:0339 (CESA-2021:0339)**
<http://lists.centos.org/pipermail/centos-announce/2021-February/048265.html>
 - RHSA-2021:0339 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:0339>
 - RHSA-2021:0183 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:0183>
 - BDU:2020-05339 (FSTEC)**
<https://bdu.fstec.ru/vul/2020-05339>
 - CVE-2020-12321 (CVE)**
CVSSv2: Базовая оценка 5.8 (AV:A/AC:L/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
NVD-CWE-noinfo
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12321>
 - RHSA-2020:5416 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:5416>
 - RHSA-2020:5479 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:5479>

Уязвимость	Риск: Высокий
ALT X ID 346076	Red Hat/CentOS -- уязвимость в sudo (CVE-2021-3156)
Описание	

В продукте sudo обнаружена уязвимость CVE-2021-3156.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:146533

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:146533>

VULN-20220110.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220110.2.pdf>

VULN-20211203.6 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20211203.6.pdf>

CESA-2021:0221 (CESA-2021:0221)

<http://lists.centos.org/pipermail/centos-announce/2021-January/048252.html>

BDU:2021-00364 (FSTEC)

<https://bdu.fstec.ru/vul/2021-00364>

CVE-2021-3156 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-193

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3156>

RHSA-2021:0227 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0227>

RHSA-2021:0218 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0218>

RHSA-2021:0221 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0221>

RHSA-2021:0226 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0226>

RHSA-2021:0219 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0219>

RHSA-2021:0220 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0220>

RHSA-2021:0222 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0222>

RHSA-2021:0223 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0223>

RHSA-2021:0225 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0225>

RHSA-2021:0224 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0224>

Уязвимость

Риск: Высокий

ALTX ID
347611

Red Hat/CentOS -- уязвимость в perl (CVE-2020-10543)

Описание

В продукте perl обнаружена уязвимость CVE-2020-10543.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:147128

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:147128>

RHSA-2021:2792 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2792>

CESA-2021:0343 (CESA-2021:0343)

<http://lists.centos.org/pipermail/centos-announce/2021-February/048259.html>

RHSA-2021:1678 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1678>

RHSA-2021:1266 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1266>

RHSA-2021:1032 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1032>

RHSA-2021:0883 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0883>

BDU:2020-04039 (FSTEC)

<https://bdu.fstec.ru/vul/2020-04039>

CVE-2020-10543 (CVE)

CVSSv2: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:N/I:P/A:P)

CVSSv3: Базовая оценка 8.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10543>

RHSA-2021:0343 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0343>

Уязвимость	Риск: Высокий
ALTX ID 347612	Red Hat/CentOS -- уязвимость в perl (CVE-2020-10878)
Описание	

В продукте perl обнаружена уязвимость CVE-2020-10878.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:147129

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:147129>

VULN-20220209.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220209.2.pdf>

VULN-20220209.1 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220209.1.pdf>

RHSA-2021:2792 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2792>

CESA-2021:0343 (CESA-2021:0343)

<http://lists.centos.org/pipermail/centos-announce/2021-February/048259.html>

RHSA-2021:1678 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1678>

RHSA-2021:1266 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1266>

RHSA-2021:1032 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1032>

RHSA-2021:0883 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0883>

BDU:2020-04040 (FSTEC)

<https://bdu.fstec.ru/vul/2020-04040>

CVE-2020-10878 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10878>

RHSA-2021:0343 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0343>

Уязвимость	Риск: Высокий
ALT X ID 348240	Red Hat/CentOS -- уязвимость в kernel (CVE-2020-29661)
Описание	

В продукте kernel обнаружена уязвимость CVE-2020-29661.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:147491

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:147491>

RHSA-2021:0774 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0774>

RHSA-2021:2164 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2164>

CESA-2021:0856 (CESA-2021:0856)

<http://lists.centos.org/pipermail/centos-announce/2021-March/048295.html>

RHSA-2021:0558 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0558>

RHSA-2021:1288 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1288>

RHSA-2021:1031 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1031>

RHSA-2021:1028 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1028>

RHSA-2021:0878 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0878>

RHSA-2021:0857 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0857>

RHSA-2021:0856 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0856>

RHSA-2021:0940 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0940>

RHSA-2021:0862 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0862>

RHSA-2021:0763 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0763>

RHSA-2021:0765 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0765>

RHSA-2021:0686 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0686>

RHSA-2021:0689 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0689>

BDU:2021-00005 (FSTEC)

<https://bdu.fstec.ru/vul/2021-00005>

CVE-2020-29661 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29661>

RHSA-2021:0537 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0537>

Уязвимость	Риск: Высокий
ALTX ID 348949	Red Hat/CentOS -- уязвимость в Bind (CVE-2020-8625)
Описание	

В продукте Bind обнаружена уязвимость CVE-2020-8625.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:147920

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:147920>

VULN-20221021.3 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221021.3.pdf>

VULN-20220906.7 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220906.7.pdf>

RHSA-2021:0922 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0922>

BDU:2021-01179 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01179>

CVE-2020-8625 (CVE)

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-120

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8625>

RHSA-2021:0672 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0672>

RHSA-2021:0671 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0671>

CESA-2021:0671 (CESA-2021:0671)

<http://lists.centos.org/pipermail/centos-announce/2021-March/048281.html>

RHSA-2021:0669 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0669>

RHSA-2021:0670 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0670>

RHSA-2021:0691 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0691>

RHSA-2021:0692 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0692>

RHSA-2021:0693 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0693>

RHSA-2021:0694 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0694>

RHSA-2021:0727 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0727>

Уязвимость	Риск: Высокий
ALTX ID 350027	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-25645)
Описание	В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-25645.
Исправление	Необходимо установить актуальное обновление от производителя.
Ссылки	oval:ru.altx-soft.nix:def:148600 https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148600 CESA-2021:0856 (CESA-2021:0856) http://lists.centos.org/pipermail/centos-announce/2021-March/048295.html BDU:2020-05383 (FSTEC) https://bdu.fstec.ru/vul/2020-05383 CVE-2020-25645 (CVE) CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N) CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) CWE-319 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25645 RHSA-2021:0857 (VENDOR) https://access.redhat.com/errata/RHSA-2021:0857 RHSA-2021:0856 (VENDOR) https://access.redhat.com/errata/RHSA-2021:0856

Уязвимость	Риск: Высокий
ALTX ID 350030	Red Hat/CentOS -- уязвимость в kernel (CVE-2020-28374)
Описание	В продукте kernel обнаружена уязвимость CVE-2020-28374.
Исправление	Необходимо установить актуальное обновление от производителя.
Ссылки	oval:ru.altx-soft.nix:def:148603 https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148603 RHSA-2021:2190 (VENDOR) https://access.redhat.com/errata/RHSA-2021:2190 RHSA-2021:2732 (VENDOR) https://access.redhat.com/errata/RHSA-2021:2732 RHSA-2021:2167 (VENDOR) https://access.redhat.com/errata/RHSA-2021:2167

RHSA-2021:2185 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2185>

RHSA-2021:2106 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2106>

RHSA-2021:2099 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2099>

CESA-2021:0856 (CESA-2021:0856)

<http://lists.centos.org/pipermail/centos-announce/2021-March/048295.html>

BDU:2021-02587 (FSTEC)

<https://bdu.fstec.ru/vul/2021-02587>

RHSA-2021:1531 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1531>

RHSA-2021:1532 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1532>

RHSA-2021:1376 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1376>

RHSA-2021:1377 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1377>

RHSA-2021:1093 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1093>

RHSA-2021:1081 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1081>

CVE-2020-28374 (CVE)

CVSSv2: Базовая оценка 5.5 (AV:N/AC:L/Au:S/C:P/I:P/A:N)

CVSSv3: Базовая оценка 8.1 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N)

CWE-22

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28374>

RHSA-2021:0857 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0857>

RHSA-2021:0856 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0856>

RHSA-2021:0862 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0862>

Уязвимость

Риск: Высокий

ALTX ID
350449

Red Hat/CentOS -- уязвимость в nettle (CVE-2021-20305)

Описание

В продукте nettle обнаружена уязвимость CVE-2021-20305.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:148876

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148876>

VULN-20220110.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220110.2.pdf>

RHSA-2021:2760 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2760>

RHSA-2021:2758 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2758>

RHSA-2021:2280 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2280>

RHSA-2021:2356 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2356>

BDU:2021-02748 (FSTEC)

<https://bdu.fstec.ru/vul/2021-02748>

CESA-2021:1145 (CESA-2021:1145)

<http://lists.centos.org/pipermail/centos-announce/2021-April/048301.html>

RHSA-2021:1246 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1246>

RHSA-2021:1245 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1245>

RHSA-2021:1206 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1206>

CVE-2021-20305 (CVE)

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20305>

RHSA-2021:1145 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1145>

Уязвимость

Риск: Высокий

ALTX ID
350458

Red Hat/CentOS -- уязвимость в kernel, kpatch-patch-4_18_0-193, kpatch-patch-4_18_0-193_1_2, kpatch-patch-4_18_0-193_6_3, kpatch-patch-4_18_0-193_13_2, kpatch-patch-4_18_0-193_14_3, kpatch-patch-4_18_0-193_19_1, kpatch-patch-4_18_0-193_28_1, kpatch-patch-4_18_0-193_29_1, kpatch-patch-4_18_0-193_37_1, kpatch-patch-4_18_0-193_40_1, kpatch-patch-4_18_0-193_41_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-3_10_0-957_54_1, kpatch-patch-3_10_0-957_56_1, kpatch-patch-3_10_0-957_58_2, kpatch-patch-3_10_0-957_61_1, kpatch-patch-3_10_0-957_61_2, kpatch-patch-3_10_0-957_62_1, kpatch-patch-3_10_0-957_65_1, kpatch-patch-3_10_0-957_66_1, kpatch-patch-3_10_0-957_70_1, kpatch-patch-3_10_0-1062_26_1 (CVE-2021-27365)

Описание

В продукте kernel, kpatch-patch-4_18_0-193, kpatch-patch-4_18_0-193_1_2, kpatch-patch-4_18_0-193_6_3, kpatch-patch-4_18_0-193_13_2, kpatch-patch-4_18_0-193_14_3, kpatch-patch-4_18_0-193_19_1, kpatch-patch-4_18_0-193_28_1, kpatch-patch-4_18_0-193_29_1, kpatch-patch-4_18_0-193_37_1, kpatch-patch-4_18_0-193_40_1, kpatch-patch-4_18_0-193_41_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-3_10_0-957_54_1, kpatch-patch-3_10_0-957_56_1, kpatch-patch-3_10_0-957_58_2, kpatch-patch-3_10_0-957_61_1, kpatch-patch-3_10_0-957_61_2, kpatch-patch-3_10_0-957_62_1, kpatch-patch-3_10_0-957_65_1, kpatch-patch-3_10_0-957_66_1, kpatch-patch-3_10_0-957_70_1, kpatch-patch-3_10_0-1062_26_1 обнаружена уязвимость CVE-2021-27365.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:148885

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148885>

RHSA-2021:1279 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1279>

RHSA-2021:1531 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1531>

RHSA-2021:1532 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1532>

RHSA-2021:1272 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1272>

RHSA-2021:1373 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1373>

RHSA-2021:1376 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1376>

RHSA-2021:1377 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1377>

RHSA-2021:1267 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1267>

RHSA-2021:1288 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1288>

RHSA-2021:1289 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1289>

RHSA-2021:1295 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1295>

CESA-2021:1071 (CESA-2021:1071)

<http://lists.centos.org/pipermail/centos-announce/2021-April/048298.html>

RHSA-2021:1173 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1173>

RHSA-2021:1171 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1171>

RHSA-2021:1093 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1093>

BDU:2021-01666 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01666>

BDU:2021-01218 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01218>

CVE-2021-27365 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27365>

RHSA-2021:1069 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1069>

RHSA-2021:1081 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1081>

RHSA-2021:1071 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1071>

RHSA-2021:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1070>

Уязвимость	Риск: Высокий
ALT X ID 359156	Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-24489)

Описание

В продукте microcode_ctl обнаружена уязвимость CVE-2020-24489.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:155074

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:155074>

- RHSA-2021:3364 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3364>
- RHSA-2021:3322 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3322>
- RHSA-2021:2304 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2304>
- RHSA-2021:2305 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2305>
- RHSA-2021:2308 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2308>
- RHSA-2021:3317 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3317>
- RHSA-2021:3323 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3323>
- RHSA-2021:3176 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3176>
- RHSA-2021:3255 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3255>
- RHSA-2021:3028 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3028>
- CESA-2021:3028 (CESA-2021:3028)**
<http://lists.centos.org/pipermail/centos-announce/2021-August/048347.html>
- RHSA-2021:3029 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3029>
- RHSA-2021:3027 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3027>
- BDU:2021-03391 (FSTEC)**
<https://bdu.fstec.ru/vul/2021-03391>
- CVE-2020-24489 (CVE)**
CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)
CWE-459
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24489>
- RHSA-2021:2300 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2300>
- RHSA-2021:2299 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2299>
- RHSA-2021:2301 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2301>
- RHSA-2021:2302 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2302>
- RHSA-2021:2306 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2306>
- RHSA-2021:2303 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2303>
- RHSA-2021:2307 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2307>

Уязвимость	Риск: Высокий
ALTX ID 359165	Red Hat/CentOS -- уязвимость в DHCP (CVE-2021-25217)
Описание	

В продукте DHCP обнаружена уязвимость CVE-2021-25217.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:155083

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:155083>

BDU:2021-03707 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03707>

CESA-2021:2357 (CESA-2021:2357)

<http://lists.centos.org/pipermail/centos-announce/2021-June/048334.html>

RHSA-2021:2405 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2405>

RHSA-2021:2414 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2414>

RHSA-2021:2415 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2415>

RHSA-2021:2416 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2416>

RHSA-2021:2418 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2418>

RHSA-2021:2419 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2419>

RHSA-2021:2420 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2420>

RHSA-2021:2469 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2469>

CVE-2021-25217 (CVE)

CVSSv2: Базовая оценка 3.2 (AV:A/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.4 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)

CWE-119

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25217>

RHSA-2021:2359 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2359>

RHSA-2021:2357 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2357>

Уязвимость

Риск: Высокий

ALT X ID
361759

Red Hat/CentOS -- уязвимость в kpatch-patch-4_18_0-305, kernel-rt, kernel, kpatch-patch-4_18_0-147_24_2, kpatch-patch-4_18_0-193_13_2, kpatch-patch-3_10_0-1160, kpatch-patch-3_10_0-1062_30_1, kpatch-patch-3_10_0-957_58_2 (CVE-2021-33034)

Описание

В продукте kpatch-patch-4_18_0-305, kernel-rt, kernel, kpatch-patch-4_18_0-147_24_2, kpatch-patch-4_18_0-193_13_2, kpatch-patch-3_10_0-1160, kpatch-patch-3_10_0-1062_30_1, kpatch-patch-3_10_0-957_58_2 обнаружена уязвимость CVE-2021-33034.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:156246

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:156246>

- RHSA-2021:2719 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2719>
- BDU:2021-04839 (FSTEC)**
<https://bdu.fstec.ru/vul/2021-04839>
- RHSA-2021:2730 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2730>
- RHSA-2021:2733 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2733>
- RHSA-2021:2734 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2734>
- RHSA-2021:2720 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2720>
- RHSA-2021:2727 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2727>
- RHSA-2021:2732 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2732>
- RHSA-2021:2726 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2726>
- RHSA-2021:2725 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2725>
- CESA-2021:2725 (CESA-2021:2725)**
<http://lists.centos.org/pipermail/centos-announce/2021-July/048344.html>
- RHSA-2021:2718 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2718>
- RHSA-2021:2729 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2729>
- RHSA-2021:2731 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2731>
- RHSA-2021:2728 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2728>
- RHSA-2021:2666 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2666>
- RHSA-2021:2668 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2668>
- RHSA-2021:2570 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2570>
- CVE-2021-33034 (CVE)**
CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/II:P/A:P)
CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CWE-416
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33034>
- RHSA-2021:2563 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2563>
- RHSA-2021:2599 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2599>

Уязвимость	Риск: Высокий
ALT X ID	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2021-33033)
364176	
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2021-33033.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:158182

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:158182>

RHSA-2021:4140 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4140>

RHSA-2021:4356 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4356>

BDU:2021-04828 (FSTEC)

<https://bdu.fstec.ru/vul/2021-04828>

CVE-2021-33033 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33033>

RHSA-2021:2726 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2726>

RHSA-2021:2725 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2725>

CESA-2021:2725 (CESA-2021:2725)

<http://lists.centos.org/pipermail/centos-announce/2021-July/048344.html>

Уязвимость

Риск: Высокий

ALTX ID

364177

Red Hat/CentOS -- уязвимость в kernel, kpatch-patch-4_18_0-193_13_2, kpatch-patch-3_10_0-1160, kpatch-patch-4_18_0-147_24_2, kpatch-patch-4_18_0-305, kernel-rt, kpatch-patch-3_10_0-1062_30_1, kpatch-patch-3_10_0-957_58_2 (CVE-2021-33909)

Описание

В продукте kernel, kpatch-patch-4_18_0-193_13_2, kpatch-patch-3_10_0-1160, kpatch-patch-4_18_0-147_24_2, kpatch-patch-4_18_0-305, kernel-rt, kpatch-patch-3_10_0-1062_30_1, kpatch-patch-3_10_0-957_58_2 обнаружена уязвимость CVE-2021-33909.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:158183

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:158183>

RHSA-2021:2719 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2719>

BDU:2021-03848 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03848>

VULN-20210722.5 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20210722.5.pdf>

CVE-2021-33909 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33909>

RHSA-2021:2730 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2730>

RHSA-2021:2733 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2733>

RHSA-2021:2734 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2734>

RHSA-2021:2735 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2735>

RHSA-2021:2720 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2720>

RHSA-2021:2727 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2727>

RHSA-2021:2723 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2723>

RHSA-2021:2716 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2716>

RHSA-2021:2715 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2715>

RHSA-2021:2722 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2722>

RHSA-2021:2714 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2714>

RHSA-2021:2732 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2732>

RHSA-2021:2726 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2726>

RHSA-2021:2725 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2725>

CESA-2021:2725 (CESA-2021:2725)

<http://lists.centos.org/pipermail/centos-announce/2021-July/048344.html>

RHSA-2021:2718 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2718>

RHSA-2021:2729 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2729>

RHSA-2021:2731 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2731>

RHSA-2021:2728 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2728>

Уязвимость	Риск: Высокий
ALTX ID 365759	Red Hat/CentOS -- уязвимость в kpatch-patch-3_10_0-1062_36_1, kernel, kpatch-patch-3_10_0-957_61_1, kernel-rt, kpatch-patch-4_18_0-193_19_1, kpatch-patch-3_10_0-1160, kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-305 (CVE-2021-22555)

Описание

В продукте kpatch-patch-3_10_0-1062_36_1, kernel, kpatch-patch-3_10_0-957_61_1, kernel-rt, kpatch-patch-4_18_0-193_19_1, kpatch-patch-3_10_0-1160, kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-305 обнаружена уязвимость CVE-2021-22555.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:159351

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:159351>

RHSA-2021:3375 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3375>

RHSA-2021:3523 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3523>

RHSA-2021:3522 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3522>

RHSA-2021:3725 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3725>

RHSA-2021:3812 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3812>

RHSA-2021:3814 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3814>

RHSA-2021:3328 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3328>

RHSA-2021:3363 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3363>

RHSA-2021:3380 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3380>

RHSA-2021:3381 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3381>

RHSA-2021:3399 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3399>

RHSA-2021:3327 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3327>

CESA-2021:3327 (CESA-2021:3327)

<http://lists.centos.org/pipermail/centos-announce/2021-August/060904.html>

RHSA-2021:3321 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3321>

VULN-20211206.4 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20211206.4.pdf>

BDU:2021-04260 (FSTEC)

<https://bdu.fstec.ru/vul/2021-04260>

RHSA-2021:3181 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3181>

RHSA-2021:3173 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3173>

CVE-2021-22555 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22555>

RHSA-2021:3057 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3057>

RHSA-2021:3088 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3088>

RHSA-2021:3044 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3044>

Уязвимость

Риск: Высокий

ALTX ID
370722

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2021-3653)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2021-3653.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:162877

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:162877>

RHSA-2021:3909 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3909>

BDU:2022-00682 (FSTEC)

<https://bdu.fstec.ru/vul/2022-00682>

RHSA-2021:3547 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3547>

RHSA-2021:3548 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3548>

RHSA-2021:3767 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3767>

RHSA-2021:3676 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3676>

RHSA-2021:3801 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3801>

CESA-2021:3801 (CESA-2021:3801)

<http://lists.centos.org/pipermail/centos-announce/2021-November/060946.html>

RHSA-2021:3802 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3802>

RHSA-2021:3812 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3812>

RHSA-2021:4768 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4768>

RHSA-2021:4692 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4692>

CVE-2021-3653 (CVE)

CVSSv2: Базовая оценка 6.0 (AV:L/AC:L/Au:N/C:P/I:P/A:C)

CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)

CWE-862

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3653>

RHSA-2021:3904 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3904>

RHSA-2021:3987 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3987>

Уязвимость

Риск: Высокий

ALTX ID

370723

Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2021-3656)

Описание

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2021-3656.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:162878

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:162878>

RHSA-2021:3909 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3909>

BDU:2022-00683 (FSTEC)

<https://bdu.fstec.ru/vul/2022-00683>

RHSA-2021:3676 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3676>

RHSA-2021:3801 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3801>

CESA-2021:3801 (CESA-2021:3801)

<http://lists.centos.org/pipermail/centos-announce/2021-November/060946.html>

RHSA-2021:3802 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3802>

RHSA-2021:3812 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3812>

RHSA-2021:4088 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4088>

RHSA-2021:4056 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4056>

CVE-2021-3656 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)

CWE-862

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3656>

RHSA-2021:3904 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3904>

RHSA-2021:3987 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3987>

Уязвимость

Риск: Высокий

ALT X ID
370724

Red Hat/CentOS -- уязвимость в kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-193_19_1, kernel, kpatch-patch-3_10_0-1160_11_1, kpatch-patch-3_10_0-957_61_1, kpatch-patch-3_10_0-1062_40_1 (CVE-2021-37576)

Описание

В продукте kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-193_19_1, kernel, kpatch-patch-3_10_0-1160_11_1, kpatch-patch-3_10_0-957_61_1, kpatch-patch-3_10_0-1062_40_1 обнаружена уязвимость CVE-2021-37576.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:162879

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:162879>

RHSA-2021:3442 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3442>

RHSA-2021:3443 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3443>

RHSA-2021:3444 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3444>

RHSA-2021:3446 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3446>

RHSA-2021:3447 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3447>

RHSA-2021:3725 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3725>

RHSA-2021:3766 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3766>

RHSA-2021:3768 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3768>

RHSA-2021:3801 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3801>

CESA-2021:3801 (CESA-2021:3801)

<http://lists.centos.org/pipermail/centos-announce/2021-November/060946.html>

RHSA-2021:3812 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3812>

RHSA-2021:3814 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3814>

BDU:2021-04028 (FSTEC)

<https://bdu.fstec.ru/vul/2021-04028>

CVE-2021-37576 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37576>

RHSA-2021:3987 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3987>

RHSA-2021:4000 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4000>

Уязвимость	Риск: Высокий
ALTX ID 371484	Red Hat/CentOS -- уязвимость в binutils, gcc-toolset-10-gcc, gcc-toolset-11-gcc, gcc-toolset-10-annobin, rust-toolset:rhel8, annobin, gcc-toolset-11-binutils, gcc-toolset-10-binutils, llvm-toolset:rhel8, gcc-toolset-11-annobin, gcc (CVE-2021-42574)

Описание

В продукте binutils, gcc-toolset-10-gcc, gcc-toolset-11-gcc, gcc-toolset-10-annobin, rust-toolset:rhel8, annobin, gcc-toolset-11-binutils, gcc-toolset-10-binutils, llvm-toolset:rhel8, gcc-toolset-11-annobin, gcc обнаружена уязвимость CVE-2021-42574.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:163474

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:163474>

BDU:2021-05328 (FSTEC)

<https://bdu.fstec.ru/vul/2021-05328>

CESA-2021:4033 (CESA-2021:4033)

<http://lists.centos.org/pipermail/centos-announce/2021-November/048395.html>

RHSA-2021:4743 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4743>

RHSA-2021:4649 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4649>

RHSA-2021:4591 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4591>

RHSA-2021:4587 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4587>

CVE-2021-42574 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.3 (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H)

CWE-94

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42574>

- RHSA-2021:4036 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4036>
- RHSA-2021:4037 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4037>
- RHSA-2021:4038 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4038>
- RHSA-2021:4035 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4035>
- RHSA-2021:4034 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4034>
- RHSA-2021:4033 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4033>
- RHSA-2021:4585 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4585>
- RHSA-2021:4586 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4586>
- RHSA-2021:4589 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4589>
- RHSA-2021:4590 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4590>
- RHSA-2021:4592 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4592>
- RHSA-2021:4593 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4593>
- RHSA-2021:4594 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4594>
- RHSA-2021:4595 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4595>
- RHSA-2021:4596 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4596>
- RHSA-2021:4598 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4598>
- RHSA-2021:4588 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4588>
- RHSA-2021:4599 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4599>
- RHSA-2021:4600 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4600>
- RHSA-2021:4602 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4602>
- RHSA-2021:4601 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4601>

Уязвимость	Риск: Высокий
ALT X ID 377414	Red Hat/CentOS -- уязвимость в libx11 (CVE-2021-31535)
Описание	В продукте libx11 обнаружена уязвимость CVE-2021-31535.
Исправление	Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:167765

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:167765>

RHSA-2021:3296 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3296>

CESA-2021:3296 (CESA-2021:3296)

<http://lists.centos.org/pipermail/centos-announce/2021-August/060902.html>

BDU:2021-02747 (FSTEC)

<https://bdu.fstec.ru/vul/2021-02747>

CVE-2021-31535 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-120

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31535>

RHSA-2021:4326 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4326>

Уязвимость

Риск: Высокий

ALTX ID
378727

Red Hat/CentOS -- уязвимость в httpd:2.4, httpd (CVE-2021-26691)

Описание

В продуктах httpd:2.4, httpd обнаружена уязвимость CVE-2021-26691.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:168876

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:168876>

CESA-2022:0143 (CESA-2022:0143)

<http://lists.centos.org/pipermail/centos-announce/2022-January/073551.html>

RHSA-2022:0143 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0143>

BDU:2021-03678 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03678>

CVE-2021-26691 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26691>

RHSA-2021:3816 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3816>

Уязвимость

Риск: Высокий

ALTX ID
378765

Red Hat/CentOS -- уязвимость в httpd, httpd:2.4 (CVE-2021-40438)

Описание

В продуктах httpd, httpd:2.4 обнаружена уязвимость CVE-2021-40438.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:168914

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:168914>

VULN-20220914.14 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220914.14.pdf>

VULN-20220812.3 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220812.3.pdf>

VULN-20220426.6 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220426.6.pdf>

VULN-20220124.15 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220124.15.pdf>

BDU:2021-04820 (FSTEC)

<https://bdu.fstec.ru/vul/2021-04820>

CVE-2021-40438 (CVE)

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.0 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)

CWE-918

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40438>

RHSA-2021:3856 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3856>

CESA-2021:3856 (CESA-2021:3856)

<http://lists.centos.org/pipermail/centos-announce/2021-November/060939.html>

RHSA-2021:3837 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3837>

RHSA-2021:3836 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3836>

RHSA-2021:3816 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3816>

Уязвимость

Риск: Высокий

ALTX ID

379781

Red Hat/CentOS -- уязвимость в httpd:2.4, httpd (CVE-2021-39275)

Описание

В продуктах httpd:2.4, httpd обнаружена уязвимость CVE-2021-39275.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:169468

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:169468>

RHSA-2022:0891 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0891>

BDU:2022-00203 (FSTEC)

<https://bdu.fstec.ru/vul/2022-00203>

CESA-2022:0143 (CESA-2022:0143)

<http://lists.centos.org/pipermail/centos-announce/2022-January/073551.html>

CVE-2021-39275 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-787
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39275>

RHSA-2022:0143 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0143>

Уязвимость	Риск: Высокий
ALTX ID 379793	Red Hat/CentOS -- уязвимость в httpd:2.4, httpd (CVE-2021-44790)
Описание	

В продуктах httpd:2.4, httpd обнаружена уязвимость CVE-2021-44790.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:169480
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:169480>

RHSA-2022:0288 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:0288>

VULN-20221005.10 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

VULN-20220901.5 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220901.5.pdf>

VULN-20211224.15 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20211224.15.pdf>

RHSA-2022:1136 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:1136>

RHSA-2022:1137 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:1137>

RHSA-2022:1138 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:1138>

RHSA-2022:1139 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:1139>

BDU:2021-06392 (FSTEC)
<https://bdu.fstec.ru/vul/2021-06392>

CESA-2022:0143 (CESA-2022:0143)
<http://lists.centos.org/pipermail/centos-announce/2022-January/073551.html>

RHSA-2022:0258 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:0258>

CVE-2021-44790 (CVE)
CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-787
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44790>

RHSA-2022:0143 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0143>

Уязвимость	Риск: Высокий
-------------------	---------------

ALTX ID

380094

Red Hat/CentOS -- уязвимость в polkit (CVE-2021-4034)

Описание

В продукте polkit обнаружена уязвимость CVE-2021-4034.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:169757

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:169757>

RHSA-2022:0268 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0268>

VULN-20220209.3 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220209.3.pdf>

VULN-20220127.1 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220127.1.pdf>

BDU:2022-00488 (FSTEC)

<https://bdu.fstec.ru/vul/2022-00488>

CVE-2021-4034 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4034>

RHSA-2022:0272 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0272>

RHSA-2022:0271 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0271>

RHSA-2022:0270 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0270>

RHSA-2022:0269 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0269>

RHSA-2022:0267 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0267>

RHSA-2022:0266 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0266>

RHSA-2022:0265 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0265>

RHSA-2022:0273 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0273>

RHSA-2022:0274 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0274>

CESA-2022:0274 (CESA-2022:0274)

<http://lists.centos.org/pipermail/centos-announce/2022-January/073552.html>

Уязвимость

Риск: Высокий

ALTX ID

382894

Red Hat/CentOS -- уязвимость в cyrus-sasl (CVE-2022-24407)

Описание

В продукте cyrus-sasl обнаружена уязвимость CVE-2022-24407.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:171463

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:171463>

RHSA-2022:0730 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0730>

VULN-20221005.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

VULN-20220901.9 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220901.9.pdf>

VULN-20220901.7 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220901.7.pdf>

VULN-20220812.7 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220812.7.pdf>

VULN-20220803.12 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220803.12.pdf>

VULN-20220727.12 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.12.pdf>

VULN-20220624.3 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220624.3.pdf>

VULN-20220524.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220524.10.pdf>

VULN-20220516.15 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220516.15.pdf>

VULN-20220412.4 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220412.4.pdf>

BDU:2022-01443 (FSTEC)

<https://bdu.fstec.ru/vul/2022-01443>

VULN-20220318.3 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220318.3.pdf>

VULN-20220318.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220318.2.pdf>

RHSA-2022:0780 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0780>

CESA-2022:0666 (CESA-2022:0666)

<http://lists.centos.org/pipermail/centos-announce/2022-February/073559.html>

RHSA-2022:0731 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0731>

VULN-20220224.12 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220224.12.pdf>

CVE-2022-24407 (CVE)

CVSSv2: Базовая оценка 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-89

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24407>

RHSA-2022:0658 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0658>

RHSA-2022:0666 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0666>

RHSA-2022:0668 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0668>

Уязвимость

Риск: Высокий

ALTX ID
383731**Red Hat/CentOS -- уязвимость в firefox, thunderbird, expat, xmlrpc-c (CVE-2022-25235)****Описание**

В продукте firefox, thunderbird, expat, xmlrpc-c обнаружена уязвимость CVE-2022-25235.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:172036**<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:172036>**RHSA-2022:0815 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0815>**RHSA-2022:0847 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0847>**RHSA-2022:1068 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1068>**RHSA-2022:1539 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1539>**RHSA-2022:1643 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1643>**VULN-20221005.10 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>**VULN-20220901.7 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220901.7.pdf>**VULN-20220901.10 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220901.10.pdf>**VULN-20220803.6 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220803.6.pdf>**VULN-20220803.12 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220803.12.pdf>**VULN-20220727.5 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220727.5.pdf>**VULN-20220727.11 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220727.11.pdf>**VULN-20220602.3 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220602.3.pdf>**VULN-20220516.15 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220516.15.pdf>**RHSA-2022:1540 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1540>**RHSA-2022:1644 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1644>**RHSA-2022:1309 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1309>**VULN-20220412.4 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220412.4.pdf>**VULN-20220222.12 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220222.12.pdf>

CESA-2022:0824 (CESA-2022:0824)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073578.html>

CESA-2022:0850 (CESA-2022:0850)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073579.html>

RHSA-2022:1069 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1069>

CESA-2022:1069 (CESA-2022:1069)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073580.html>

RHSA-2022:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1070>

RHSA-2022:1012 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1012>

RHSA-2022:0843 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0843>

RHSA-2022:0853 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0853>

RHSA-2022:0850 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0850>

RHSA-2022:0845 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0845>

RHSA-2022:0951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0951>

VULN-20220228.4 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220228.4.pdf>

BDU:2022-01063 (FSTEC)

<https://bdu.fstec.ru/vul/2022-01063>

CVE-2022-25235 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-116

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25235>

RHSA-2022:0817 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0817>

RHSA-2022:0816 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0816>

RHSA-2022:0818 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0818>

RHSA-2022:0824 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0824>

Уязвимость

Риск: Высокий

ALTX ID
383733

Red Hat/CentOS -- уязвимость в firefox, thunderbird, expat (CVE-2022-25315)

Описание

В продуктах firefox, thunderbird, expat обнаружена уязвимость CVE-2022-25315.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:172038

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:172038>

RHSA-2022:0815 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:0815>

RHSA-2022:0847 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:0847>

RHSA-2022:1068 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:1068>

VULN-20221005.10 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

VULN-20220901.7 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220901.7.pdf>

VULN-20220901.10 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220901.10.pdf>

VULN-20220803.6 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220803.6.pdf>

VULN-20220803.13 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220803.13.pdf>

VULN-20220803.12 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220803.12.pdf>

VULN-20220727.5 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220727.5.pdf>

VULN-20220727.11 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220727.11.pdf>

VULN-20220602.3 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220602.3.pdf>

VULN-20220516.15 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220516.15.pdf>

RHSA-2022:1309 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:1309>

VULN-20220412.4 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220412.4.pdf>

VULN-20220222.12 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220222.12.pdf>

CESA-2022:0824 (CESA-2022:0824)
<http://lists.centos.org/pipermail/centos-announce/2022-March/073578.html>

CESA-2022:0850 (CESA-2022:0850)
<http://lists.centos.org/pipermail/centos-announce/2022-March/073579.html>

RHSA-2022:1069 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:1069>

CESA-2022:1069 (CESA-2022:1069)
<http://lists.centos.org/pipermail/centos-announce/2022-March/073580.html>

RHSA-2022:1070 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:1070>

RHSA-2022:1012 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:1012>

VULN-20220318.13 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220318.13.pdf>

RHSA-2022:0843 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:0843>

RHSA-2022:0853 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:0853>

RHSA-2022:0850 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:0850>

RHSA-2022:0845 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:0845>

RHSA-2022:0951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0951>

BDU:2022-01071 (FSTEC)

<https://bdu.fstec.ru/vul/2022-01071>

CVE-2022-25315 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25315>

RHSA-2022:0817 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0817>

RHSA-2022:0816 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0816>

RHSA-2022:0818 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0818>

RHSA-2022:0824 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0824>

Уязвимость	Риск: Высокий
ALTX ID 384216	Red Hat/CentOS -- уязвимость в expat (CVE-2021-45960)
Описание	

В продукте expat обнаружена уязвимость CVE-2021-45960.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:172325

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:172325>

VULN-20221005.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

VULN-20220901.7 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220901.7.pdf>

VULN-20220901.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220901.5.pdf>

VULN-20220803.6 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220803.6.pdf>

VULN-20220727.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.5.pdf>

VULN-20220118.8 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220118.8.pdf>

VULN-20220228.4 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220228.4.pdf>

RHSA-2022:1069 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1069>

CESA-2022:1069 (CESA-2022:1069)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073580.html>

BDU:2022-01003 (FSTEC)

<https://bdu.fstec.ru/vul/2022-01003>

CVE-2021-45960 (CVE)

CVSSv2: Базовая оценка 9.0 (AV:N/AC:L/Au:S/C:I/C/A:C)
CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CWE-682
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45960>

RHSA-2022:0951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0951>

Уязвимость	Риск: Высокий
ALTX ID 384217	Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2021-46143)
Описание	

В продуктах xmlrpc-c, expat обнаружена уязвимость CVE-2021-46143.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:172326
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:172326>

RHSA-2022:7692 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:7692>

VULN-20221005.10 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

VULN-20220901.7 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220901.7.pdf>

VULN-20220901.5 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220901.5.pdf>

VULN-20220803.6 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220803.6.pdf>

VULN-20220727.5 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220727.5.pdf>

VULN-20220216.10 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220216.10.pdf>

VULN-20220228.4 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220228.4.pdf>

RHSA-2022:1069 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:1069>

CESA-2022:1069 (CESA-2022:1069)
<http://lists.centos.org/pipermail/centos-announce/2022-March/073580.html>

BDU:2022-01052 (FSTEC)
<https://bdu.fstec.ru/vul/2022-01052>

CVE-2021-46143 (CVE)
CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
CWE-190
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46143>

RHSA-2022:0951 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:0951>

Уязвимость	Риск: Высокий
-------------------	---------------

ALTX ID

384219

Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2022-22822)

Описание

В продуктах xmlrpc-c, expat обнаружена уязвимость CVE-2022-22822.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:172328

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:172328>

RHSA-2022:7692 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7692>

VULN-20221005.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

VULN-20220901.7 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220901.7.pdf>

VULN-20220901.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220901.5.pdf>

VULN-20220803.6 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220803.6.pdf>

VULN-20220727.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.5.pdf>

BDU:2022-02823 (FSTEC)

<https://bdu.fstec.ru/vul/2022-02823>

VULN-20220118.8 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220118.8.pdf>

VULN-20220228.4 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220228.4.pdf>

RHSA-2022:1069 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1069>

CESA-2022:1069 (CESA-2022:1069)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073580.html>

CVE-2022-22822 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22822>

RHSA-2022:0951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0951>

Уязвимость

Риск: Высокий

ALTX ID

384220

Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2022-22823)

Описание

В продуктах xmlrpc-c, expat обнаружена уязвимость CVE-2022-22823.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:172329

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:172329>

RHSA-2022:7692 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7692>

VULN-20221005.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

VULN-20220901.7 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220901.7.pdf>

VULN-20220803.6 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220803.6.pdf>

VULN-20220727.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.5.pdf>

VULN-20220118.8 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220118.8.pdf>

VULN-20220228.4 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220228.4.pdf>

RHSA-2022:1069 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1069>

CESA-2022:1069 (CESA-2022:1069)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073580.html>

BDU:2022-01060 (FSTEC)

<https://bdu.fstec.ru/vul/2022-01060>

CVE-2022-22823 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22823>

RHSA-2022:0951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0951>

Уязвимость	Риск: Высокий
ALTX ID 384221	Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2022-22824)
Описание	

В продуктах xmlrpc-c, expat обнаружена уязвимость CVE-2022-22824.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:172330

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:172330>

RHSA-2022:7692 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7692>

VULN-20221005.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

VULN-20220901.7 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220901.7.pdf>

VULN-20220803.6 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220803.6.pdf>

VULN-20220727.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.5.pdf>

VULN-20220118.8 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220118.8.pdf>

VULN-20220228.4 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220228.4.pdf>

RHSA-2022:1069 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1069>

CESA-2022:1069 (CESA-2022:1069)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073580.html>

BDU:2022-00800 (FSTEC)

<https://bdu.fstec.ru/vul/2022-00800>

CVE-2022-22824 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22824>

RHSA-2022:0951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0951>

Уязвимость	Риск: Высокий
ALTX ID 384222	Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2022-22825)
Описание	

В продуктах xmlrpc-c, expat обнаружена уязвимость CVE-2022-22825.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:172331

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:172331>

RHSA-2022:7692 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7692>

VULN-20221005.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

VULN-20220901.7 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220901.7.pdf>

VULN-20220803.6 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220803.6.pdf>

VULN-20220727.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.5.pdf>

VULN-20220118.8 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220118.8.pdf>

VULN-20220228.4 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220228.4.pdf>

RHSA-2022:1069 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1069>

CESA-2022:1069 (CESA-2022:1069)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073580.html>

BDU:2022-00805 (FSTEC)

<https://bdu.fstec.ru/vul/2022-00805>

CVE-2022-22825 (CVE)

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
CWE-190
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22825>

RHSA-2022:0951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0951>

Уязвимость	Риск: Высокий
ALT X ID 384223	Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2022-22826)
Описание	

В продуктах xmlrpc-c, expat обнаружена уязвимость CVE-2022-22826.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:172332
<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:172332>

RHSA-2022:7692 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:7692>

VULN-20221005.10 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

VULN-20220901.7 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220901.7.pdf>

VULN-20220803.6 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220803.6.pdf>

VULN-20220727.5 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220727.5.pdf>

VULN-20220118.8 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220118.8.pdf>

VULN-20220228.4 (NKCKI)
<https://safe-surf.ru/upload/VULN/VULN-20220228.4.pdf>

RHSA-2022:1069 (VENDOR)
<https://access.redhat.com/errata/RHSA-2022:1069>

CESA-2022:1069 (CESA-2022:1069)
<http://lists.centos.org/pipermail/centos-announce/2022-March/073580.html>

BDU:2022-01059 (FSTEC)
<https://bdu.fstec.ru/vul/2022-01059>

CVE-2022-22826 (CVE)
CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
CWE-190
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22826>

RHSA-2022:0951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0951>

Уязвимость	Риск: Высокий
ALT X ID 384224	Red Hat/CentOS -- уязвимость в xmlrpc-c, expat (CVE-2022-22827)

Описание

В продуктах xmlrpc-c, expat обнаружена уязвимость CVE-2022-22827.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:172333

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:172333>

RHSA-2022:7692 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7692>

VULN-20221005.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

VULN-20220901.7 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220901.7.pdf>

VULN-20220803.6 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220803.6.pdf>

VULN-20220727.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.5.pdf>

VULN-20220118.8 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220118.8.pdf>

VULN-20220228.4 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220228.4.pdf>

RHSA-2022:1069 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1069>

CESA-2022:1069 (CESA-2022:1069)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073580.html>

BDU:2022-01058 (FSTEC)

<https://bdu.fstec.ru/vul/2022-01058>

CVE-2022-22827 (CVE)

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22827>

RHSA-2022:0951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0951>

Уязвимость

Риск: Высокий

ALTX ID

384225

Red Hat/CentOS -- уязвимость в expat (CVE-2022-23852)

Описание

В продукте expat обнаружена уязвимость CVE-2022-23852.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:172334

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:172334>

VULN-20221005.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.5.pdf>

VULN-20221005.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

VULN-20220901.7 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220901.7.pdf>

VULN-20220901.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220901.5.pdf>

VULN-20220727.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.5.pdf>

VULN-20220727.11 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.11.pdf>

RHSA-2022:4834 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:4834>

BDU:2022-01702 (FSTEC)

<https://bdu.fstec.ru/vul/2022-01702>

VULN-20220228.4 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220228.4.pdf>

RHSA-2022:1069 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1069>

CESA-2022:1069 (CESA-2022:1069)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073580.html>

VULN-20220125.9 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220125.9.pdf>

CVE-2022-23852 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23852>

RHSA-2022:0951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0951>

Уязвимость

Риск: Высокий

ALT X ID
387955

Red Hat/CentOS -- уязвимость в OpenSSL, compat-openssl10, compat-openssl11 (CVE-2022-0778)

Описание

В продуктах OpenSSL, compat-openssl10, compat-openssl11 обнаружена уязвимость CVE-2022-0778.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:175933

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:175933>

VULN-20230111.1 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20230111.1.pdf>

RHSA-2022:1112 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1112>

RHSA-2022:4899 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:4899>

RHSA-2022:5326 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:5326>

VULN-20221005.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

VULN-20220901.5 (NKCKI)<https://safe-surf.ru/upload/VULN/VULN-20220901.5.pdf>**VULN-20220803.8 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220803.8.pdf>**VULN-20220803.13 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220803.13.pdf>**VULN-20220803.12 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220803.12.pdf>**VULN-20220624.3 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220624.3.pdf>**VULN-20220621.1 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220621.1.pdf>**VULN-20220516.15 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220516.15.pdf>**VULN-20220412.4 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220412.4.pdf>**BDU:2022-01315 (FSTEC)**<https://bdu.fstec.ru/vul/2022-01315>**CVE-2022-0778 (CVE)**

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-835

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778>**RHSA-2022:1065 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1065>**RHSA-2022:1066 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1066>**CESA-2022:1066 (CESA-2022:1066)**<http://lists.centos.org/pipermail/centos-announce/2022-March/073577.html>**RHSA-2022:1071 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1071>**RHSA-2022:1073 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1073>**RHSA-2022:1076 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1076>**RHSA-2022:1077 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1077>**RHSA-2022:1078 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1078>**RHSA-2022:1082 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1082>**RHSA-2022:1091 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1091>

Уязвимость	Риск: Высокий
ALT X ID 390363	Red Hat/CentOS -- уязвимость в zlib, rsync (CVE-2018-25032)
Описание	

В продуктах zlib, rsync обнаружена уязвимость CVE-2018-25032.

Исправление	Необходимо установить актуальное обновление от производителя.
--------------------	---

Ссылки

oval:ru.altx-soft.nix:def:177533

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:177533>

VULN-20230111.1 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20230111.1.pdf>

RHSA-2022:1591 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1591>

RHSA-2022:2197 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:2197>

RHSA-2022:4592 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:4592>

RHSA-2022:4584 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:4584>

VULN-20221005.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

RHSA-2022:4845 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:4845>

CESA-2022:2213 (CESA-2022:2213)

<http://lists.centos.org/pipermail/centos-announce/2022-May/073584.html>

RHSA-2022:2192 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:2192>

RHSA-2022:2198 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:2198>

RHSA-2022:2213 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:2213>

RHSA-2022:2214 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:2214>

RHSA-2022:2201 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:2201>

RHSA-2022:1661 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1661>

BDU:2022-01641 (FSTEC)

<https://bdu.fstec.ru/vul/2022-01641>

CVE-2018-25032 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-25032>

RHSA-2022:1642 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1642>

Уязвимость

Риск: Высокий

ALTX ID

404030

Red Hat/CentOS -- уязвимость в systemd (CVE-2022-2526)

Описание

В продукте systemd обнаружена уязвимость CVE-2022-2526.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:187478

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:187478>

RHSA-2022:6163 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6163>

VULN-20221101.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221101.2.pdf>

CESA-2022:6160 (CESA-2022:6160)

<http://lists.centos.org/pipermail/centos-announce/2022-September/073636.html>

RHSA-2022:6206 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6206>

BDU:2022-05168 (FSTEC)

<https://bdu.fstec.ru/vul/2022-05168>

CVE-2022-2526 (CVE)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2526>

RHSA-2022:6162 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6162>

RHSA-2022:6161 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6161>

RHSA-2022:6160 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6160>

Уязвимость

Риск: Высокий

ALTX ID

410366

Red Hat/CentOS -- уязвимость в expat, firefox, thunderbird, compat-expat1 (CVE-2022-40674)

Описание

В продукте expat, firefox, thunderbird, compat-expat1 обнаружена уязвимость CVE-2022-40674.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:192792

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:192792>

VULN-20230201.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20230201.2.pdf>

RHSA-2022:6833 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6833>

RHSA-2022:7019 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7019>

RHSA-2022:7021 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7021>

VULN-20221110.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221110.5.pdf>

VULN-20221109.13 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221109.13.pdf>

CESA-2022:6834 (CESA-2022:6834)

<http://lists.centos.org/pipermail/centos-announce/2022-October/073647.html>

RHSA-2022:6967 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6967>

RHSA-2022:6995 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6995>

RHSA-2022:6998 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6998>

RHSA-2022:7020 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7020>

RHSA-2022:7022 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7022>

RHSA-2022:7025 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7025>

RHSA-2022:7026 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7026>

RHSA-2022:7024 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7024>

RHSA-2022:7023 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7023>

RHSA-2022:6997 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6997>

RHSA-2022:6996 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6996>

VULN-20221021.9 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221021.9.pdf>

RHSA-2022:6878 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6878>

CVE-2022-40674 (CVE)

CVSSv3: Базовая оценка 8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40674>

RHSA-2022:6831 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6831>

RHSA-2022:6832 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6832>

RHSA-2022:6838 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6838>

RHSA-2022:6834 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6834>

Уязвимость	Риск: Высокий
ALTX ID 415511	Red Hat/CentOS -- уязвимость в krb5 (CVE-2022-42898)

Описание

В продукте krb5 обнаружена уязвимость CVE-2022-42898.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:197202

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:197202>

RHSA-2022:8641 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8641>

CESA-2022:8640 (CESA-2022:8640)

<http://lists.centos.org/pipermail/centos-announce/2022-November/073665.html>

BDU:2022-06933 (FSTEC)

<https://bdu.fstec.ru/vul/2022-06933>

CVE-2022-42898 (CVE)

CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42898>

RHSA-2022:8637 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8637>

RHSA-2022:8638 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8638>

RHSA-2022:8640 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8640>

RHSA-2022:8639 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8639>

RHSA-2022:8648 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8648>

RHSA-2022:8669 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8669>

RHSA-2022:8663 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8663>

RHSA-2022:8662 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8662>

Уязвимость	Риск: Высокий
ALTX ID 419836	Red Hat/CentOS -- уязвимость в libXpm (CVE-2022-4883)
Описание	

В продукте libXpm обнаружена уязвимость CVE-2022-4883.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:200613

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:200613>

CESA-2023:0377 (CESA-2023:0377)

<http://lists.centos.org/pipermail/centos-announce/2023-January/086364.html>

BDU:2023-00388 (FSTEC)

<https://bdu.fstec.ru/vul/2023-00388>

CVE-2022-4883 (CVE)

CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4883>

RHSA-2023:0384 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0384>

RHSA-2023:0383 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0383>

RHSA-2023:0382 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0382>

RHSA-2023:0380 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0380>

RHSA-2023:0379 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0379>

RHSA-2023:0378 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0378>

RHSA-2023:0377 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0377>

Уязвимость

Риск: Высокий

ALTX ID

419838

Red Hat/CentOS -- уязвимость в sudo (CVE-2023-22809)

Описание

В продукте sudo обнаружена уязвимость CVE-2023-22809.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:200615

<https://ovaldbrn.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:200615>

CESA-2023:0291 (CESA-2023:0291)

<http://lists.centos.org/pipermail/centos-announce/2023-January/086363.html>

BDU:2023-00210 (FSTEC)

<https://bdu.fstec.ru/vul/2023-00210>

CVE-2023-22809 (CVE)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-269

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22809>

RHSA-2023:0280 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0280>

RHSA-2023:0281 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0281>

RHSA-2023:0282 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0282>

RHSA-2023:0283 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0283>

RHSA-2023:0293 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0293>

RHSA-2023:0292 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0292>

RHSA-2023:0291 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0291>

RHSA-2023:0287 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0287>

RHSA-2023:0284 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0284>

Уязвимость

Риск: Высокий

ALTX ID

421523

Red Hat/CentOS -- уязвимость в WebKitGTK (CVE-2023-23529)

Описание

В продукте WebKitGTK обнаружена уязвимость CVE-2023-23529.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:201801

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:201801>

RHSA-2023:0903 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0903>

RHSA-2023:0902 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0902>

CVE-2023-23529 (CVE)

CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

CWE-843

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23529>

CVE-2023-23529 (VENDOR)

<https://access.redhat.com/security/cve/CVE-2023-23529>

Уязвимость

Риск: Средний

ALTX ID

286967

Red Hat/CentOS -- уязвимость в dbus (CVE-2019-12749)

Описание

В продукте dbus обнаружена уязвимость CVE-2019-12749.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:103651

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:103651>

CESA-2020:4032 (CESA-2020:4032)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012677.html>

RHSA-2020:4032 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4032>

RHSA-2019:2868 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:2868>

RHSA-2019:3707 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3707>

BDU:2019-03326 (FSTEC)

<https://bdu.fstec.ru/vul/2019-03326>

RHSA-2019:2870 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:2870>

CVE-2019-12749 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:P/I:P/A:N)

CVSSv3: Базовая оценка 7.0 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-59

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12749>

RHSA-2019:1726 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:1726>

CESA-2019:1726 (CESA-2019:1726)

<http://lists.centos.org/pipermail/centos-announce/2019-July/023361.html>

Уязвимость

Риск: Средний

ALTX ID

288301

Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2019-11719)

Описание

В продуктах nspr, nss обнаружена уязвимость CVE-2019-11719.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:104414

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:104414>

CESA-2020:4076-CentOS 7 (CESA-2020:4076)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-November/012876.html>

RHSA-2020:4076 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4076>

BDU:2019-03616 (FSTEC)

<https://bdu.fstec.ru/vul/2019-03616>

CVE-2019-11719 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11719>

RHSA-2019:1951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:1951>

Уязвимость

Риск: Средний

ALTX ID

289444

Red Hat/CentOS -- уязвимость в mariadb:10.3, mariadb, mariadb-devel, MySQL (CVE-2019-2737)

Описание

В продукте mariadb:10.3, mariadb, mariadb-devel, MySQL обнаружена уязвимость CVE-2019-2737.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:105005

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:105005>

RHSA-2020:5663 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5663>

CESA-2020:1100 (CESA-2020:1100)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012528.html>

RHSA-2020:1100 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1100>

RHSA-2019:3708 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3708>

BDU:2019-03233 (FSTEC)

<https://bdu.fstec.ru/vul/2019-03233>

CVE-2019-2737 (CVE)

CVSSv2: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)
 CVSSv3: Базовая оценка 4.9 (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H)
 NVD-CWE-noinfo
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2737>

RHSA-2019:2511 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:2511>

Уязвимость	Риск: Средний
ALTX ID 289446	Red Hat/CentOS -- уязвимость в mariadb:10.3, mariadb, mariadb-devel, MySQL (CVE-2019-2739)
Описание	

В продукте mariadb:10.3, mariadb, mariadb-devel, MySQL обнаружена уязвимость CVE-2019-2739.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:105007
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:105007>

RHSA-2020:5663 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5663>

CESA-2020:1100 (CESA-2020:1100)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012528.html>

RHSA-2020:1100 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1100>

RHSA-2019:3708 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3708>

BDU:2019-03235 (FSTEC)

<https://bdu.fstec.ru/vul/2019-03235>

CVE-2019-2739 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:N/I:P/A:P)
 CVSSv3: Базовая оценка 5.0 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H)
 NVD-CWE-noinfo
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2739>

RHSA-2019:2511 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:2511>

Уязвимость	Риск: Средний
ALTX ID 289447	Red Hat/CentOS -- уязвимость в mariadb:10.3, mariadb, mariadb-devel, MySQL (CVE-2019-2740)
Описание	

В продукте mariadb:10.3, mariadb, mariadb-devel, MySQL обнаружена уязвимость CVE-2019-2740.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:105008
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:105008>

RHSA-2020:5663 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:5663>**CESA-2020:1100 (CESA-2020:1100)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012528.html>**RHSA-2020:1100 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1100>**RHSA-2019:3708 (VENDOR)**<https://access.redhat.com/errata/RHSA-2019:3708>**BDU:2019-03236 (FSTEC)**<https://bdu.fstec.ru/vul/2019-03236>**CVE-2019-2740 (CVE)**

CVSSv2: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)

CVSSv3: Базовая оценка 6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2740>**RHSA-2019:2511 (VENDOR)**<https://access.redhat.com/errata/RHSA-2019:2511>

Уязвимость

Риск: Средний

ALTX ID
289466**Red Hat/CentOS -- уязвимость в mariadb:10.3, mariadb, mariadb-devel, MySQL (CVE-2019-2805)**

Описание

В продукте mariadb:10.3, mariadb, mariadb-devel, MySQL обнаружена уязвимость CVE-2019-2805.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:105027<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:105027>**RHSA-2020:5663 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5663>**CESA-2020:1100 (CESA-2020:1100)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012528.html>**BDU:2020-01528 (FSTEC)**<https://bdu.fstec.ru/vul/2020-01528>**RHSA-2020:1100 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1100>**RHSA-2019:3708 (VENDOR)**<https://access.redhat.com/errata/RHSA-2019:3708>**CVE-2019-2805 (CVE)**

CVSSv2: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)

CVSSv3: Базовая оценка 6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2805>**RHSA-2019:2511 (VENDOR)**<https://access.redhat.com/errata/RHSA-2019:2511>

Уязвимость

Риск: Средний

ALTX ID
291917**Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-9503)**

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-9503.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:106810

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:106810>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

RHSA-2020:2522 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2522>

BDU:2020-02045 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02045>

RHSA-2020:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1070>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

RHSA-2019:2703 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:2703>

CVE-2019-9503 (CVE)

CVSSv2: Базовая оценка 7.9 (AV:A/AC:M/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 5.9 (CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:H)

CWE-20

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9503>

RHSA-2019:2741 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:2741>

Уязвимость

Риск: Средний

ALTX ID
307173

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2018-19985)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2018-19985.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:120758

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:120758>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

RHSA-2020:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1070>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

RHSA-2019:3517 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3517>

BDU:2019-01409 (FSTEC)

<https://bdu.fstec.ru/vul/2019-01409>

CVE-2018-19985 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 4.5 (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-125
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19985>

RHSA-2019:3309 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3309>

Уязвимость	Риск: Средний
ALT X ID 307174	Red Hat/CentOS -- уязвимость в kernel-rt, kernel, perf, kernel-debug, kernel-debug-devel, kernel-devel, kernel-doc, kernel-headers, kernel-abi-whitelists, kernel-tools, kernel-tools-libs, kernel-tools-libs-devel, python-perf (CVE-2018-20169)

Описание

В продукте kernel-rt, kernel, perf, kernel-debug, kernel-debug-devel, kernel-devel, kernel-doc, kernel-headers, kernel-abi-whitelists, kernel-tools, kernel-tools-libs, kernel-tools-libs-devel, python-perf обнаружена уязвимость CVE-2018-20169.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

- oval:ru.altx-soft.nix:def:120759
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:120759>
- CESA-2020:1016 (CESA-2020:1016)
<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>
- RHSA-2020:2522 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:2522>
- RHSA-2020:2770 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:2770>
- RHSA-2020:2851 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:2851>
- RHSA-2020:1070 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:1070>
- RHSA-2020:1016 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:1016>
- RHSA-2019:3517 (VENDOR)
<https://access.redhat.com/errata/RHSA-2019:3517>
- BDU:2019-02380 (FSTEC)
<https://bdu.fstec.ru/vul/2019-02380>
- CVE-2018-20169 (CVE)**
CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
CVSSv3: Базовая оценка 6.4 (CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-400
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20169>
- RHSA-2019:3309 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2019:3309>

Уязвимость	Риск: Средний
ALT X ID 307177	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-10207)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-10207.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:120762

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:120762>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

RHSA-2020:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1070>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

RHSA-2019:3517 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3517>

BDU:2019-04744 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04744>

CVE-2019-10207 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 4.6 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10207>

RHSA-2019:3309 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3309>

Уязвимость

Риск: Средний

ALTX ID

307183

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-11884)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-11884.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:120768

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:120768>

BDU:2021-03082 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03082>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

RHSA-2020:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1070>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

RHSA-2019:3517 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3517>

CVE-2019-11884 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 6.8 (CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11884>

RHSA-2019:3309 (VENDOR)<https://access.redhat.com/errata/RHSA-2019:3309>

Уязвимость	Риск: Средний
ALTX ID 307185	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-13233)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-13233.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:120770

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:120770>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

RHSA-2020:2522 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2522>

RHSA-2020:2851 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2851>

RHSA-2020:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1070>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

RHSA-2019:3517 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3517>

BDU:2019-02751 (FSTEC)

<https://bdu.fstec.ru/vul/2019-02751>

CVE-2019-13233 (CVE)

CVSSv2: Базовая оценка 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 5.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CWE-362

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13233>

RHSA-2019:3309 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3309>

Уязвимость	Риск: Средний
ALTX ID 307211	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-15916)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-15916.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:120796

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:120796>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

RHSA-2020:2522 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2522>

RHSA-2020:2851 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2851>

BDU:2020-04876 (FSTEC)

<https://bdu.fstec.ru/vul/2020-04876>

RHSA-2020:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1070>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

RHSA-2019:3517 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3517>

CVE-2019-15916 (CVE)

CVSSv2: Базовая оценка 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15916>

RHSA-2019:3309 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3309>

Уязвимость	Риск: Средний
ALTX ID 316326	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-14898)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-14898.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:126765

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:126765>

CESA-2020:0375 (CESA-2020:0375)

<http://lists.centos.org/pipermail/centos-announce/2020-February/035620.html>

CESA-2020:0374 (CESA-2020:0374)

<http://lists.centos.org/pipermail/centos-announce/2020-February/035645.html>

BDU:2020-02253 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02253>

RHSA-2020:0374 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0374>

CVE-2019-14898 (CVE)

CVSSv2: Базовая оценка 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.0 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-362

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14898>

RHSA-2020:0375 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0375>

RHSA-2020:0339 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0339>

RHSA-2020:0328 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0328>

Уязвимость

Риск: Средний

ALTX ID
316331

Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2019-17666)

Описание

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2019-17666.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:126770

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:126770>

CESA-2020:0839 (CESA-2020:0839)

<http://lists.centos.org/pipermail/centos-announce/2020-March/035660.html>

CESA-2020:1524 (CESA-2020:1524)

<http://lists.centos.org/pipermail/centos-announce/2020-April/035703.html>

RHSA-2020:1465 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1465>

RHSA-2020:1473 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1473>

RHSA-2020:1347 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1347>

RHSA-2020:1524 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1524>

RHSA-2020:0834 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0834>

RHSA-2020:0661 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0661>

RHSA-2020:0839 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0839>

RHSA-2020:0543 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0543>

BDU:2019-03812 (FSTEC)

<https://bdu.fstec.ru/vul/2019-03812>

CVE-2019-17666 (CVE)

CVSSv2: Базовая оценка 8.3 (AV:A/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 6.3 (CVSS:3.0/AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H)

CWE-120

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17666>

RHSA-2020:0339 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0339>

RHSA-2020:0328 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0328>

Уязвимость

Риск: Средний

ALTX ID
316332

Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2019-19338)

Описание

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2019-19338.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:126771

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:126771>

CESA-2020:0839 (CESA-2020:0839)

<http://lists.centos.org/pipermail/centos-announce/2020-March/035660.html>

RHSA-2020:1465 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1465>

RHSA-2020:0834 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0834>

RHSA-2020:0839 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0839>

CVE-2019-19338 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CWE-203

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19338>

RHSA-2020:0339 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0339>

RHSA-2020:0328 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:0328>

Уязвимость

Риск: Средний

ALTX ID

317741

Red Hat/CentOS -- уязвимость в Bind (CVE-2018-5745)

Описание

В продукте Bind обнаружена уязвимость CVE-2018-5745.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:127627

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:127627>

CESA-2020:1061 (CESA-2020:1061)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012415.html>

RHSA-2020:1061 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1061>

BDU:2020-00773 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00773>

CVE-2018-5745 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:N/AC:M/Au:S/C:N/I:N/A:P)

CVSSv3: Базовая оценка 4.9 (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H)

CWE-327

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5745>

RHSA-2019:3552 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3552>

Уязвимость

Риск: Средний

ALTX ID
317751

Red Hat/CentOS -- уязвимость в glib2, ibus (CVE-2019-12450)

Описание

В продуктах glib2, ibus обнаружена уязвимость CVE-2019-12450.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:127637

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:127637>

RHSA-2020:3978 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3978>

CESA-2020:3978-CentOS 7 (CESA-2020:3978)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012712.html>

BDU:2019-04780 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04780>

CVE-2019-12450 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 6.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N)

CWE-362

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12450>

RHSA-2019:3530 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3530>

Уязвимость

Риск: Средний

ALTX ID
317763

Red Hat/CentOS -- уязвимость в dovecot (CVE-2019-3814)

Описание

В продукте dovecot обнаружена уязвимость CVE-2019-3814.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:127649

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:127649>

CESA-2020:1062 (CESA-2020:1062)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012433.html>

RHSA-2020:1062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1062>

BDU:2019-01416 (FSTEC)

<https://bdu.fstec.ru/vul/2019-01416>

CVE-2019-3814 (CVE)

CVSSv2: Базовая оценка 4.9 (AV:N/AC:M/Au:S/C:P/I:P/A:N)

CVSSv3: Базовая оценка 7.6 (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:N)

CWE-295

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-3814>

RHSA-2019:3467 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3467>

Уязвимость	Риск: Средний
ALTX ID 320064	Red Hat/CentOS -- уязвимость в httpd (CVE-2017-15710)
Описание	В продукте httpd обнаружена уязвимость CVE-2017-15710.
Исправление	Необходимо установить актуальное обновление от производителя.
Ссылки	oval:ru.altx-soft.nix:def:129112 https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129112 CESA-2020:1121 (CESA-2020:1121) http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012463.html BDU:2019-04105 (FSTEC) https://bdu.fstec.ru/vul/2019-04105 CVE-2017-15710 (CVE) CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P) CVSSv3: Базовая оценка 5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H) CWE-787 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15710 RHSA-2020:1121 (VENDOR) https://access.redhat.com/errata/RHSA-2020:1121

Уязвимость	Риск: Средний
ALTX ID 320072	Red Hat/CentOS -- уязвимость в avahi (CVE-2017-6519)
Описание	В продукте avahi обнаружена уязвимость CVE-2017-6519.
Исправление	Необходимо установить актуальное обновление от производителя.
Ссылки	oval:ru.altx-soft.nix:def:129120 https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129120 CESA-2020:1176 (CESA-2020:1176) http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012411.html BDU:2019-00693 (FSTEC) https://bdu.fstec.ru/vul/2019-00693 CVE-2017-6519 (CVE) CVSSv2: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P) CVSSv3: Базовая оценка 5.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L) CWE-346 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6519 RHSA-2020:1176 (VENDOR) https://access.redhat.com/errata/RHSA-2020:1176

Уязвимость	Риск: Средний
-------------------	---------------

ALTX ID
320078

Red Hat/CentOS -- уязвимость в file, file-devel, file-libs, file-static, python-magic (CVE-2018-10360)

Описание

В продукте file, file-devel, file-libs, file-static, python-magic обнаружена уязвимость CVE-2018-10360.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129126

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129126>

CESA-2020:1022 (CESA-2020:1022)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012446.html>

RHSA-2020:2521 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2521>

RHSA-2020:2768 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2768>

RHSA-2020:2838 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2838>

BDU:2018-01425 (FSTEC)

<https://bdu.fstec.ru/vul/2018-01425>

CVE-2018-10360 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 5.4 (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10360>

RHSA-2020:1022 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1022>

Уязвимость

Риск: Средний

ALTX ID
320079

Red Hat/CentOS -- уязвимость в php (CVE-2018-10547)

Описание

В продукте php обнаружена уязвимость CVE-2018-10547.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129127

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129127>

CESA-2020:1112 (CESA-2020:1112)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012562.html>

BDU:2019-04235 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04235>

CVE-2018-10547 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 6.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CWE-79

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10547>

RHSA-2020:1112 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:1112>

Уязвимость	Риск: Средний
ALTX ID 320098	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2018-14404)
Описание	

В продукте libxml2 обнаружена уязвимость CVE-2018-14404.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:129146**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129146>**CESA-2020:1190 (CESA-2020:1190)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012518.html>**RHSA-2020:1827 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1827>**BDU:2019-00518 (FSTEC)**<https://bdu.fstec.ru/vul/2019-00518>**CVE-2018-14404 (CVE)**

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14404>**RHSA-2020:1190 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1190>

Уязвимость	Риск: Средний
ALTX ID 320103	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2018-14567)
Описание	

В продукте libxml2 обнаружена уязвимость CVE-2018-14567.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:129151**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129151>**CESA-2020:1190 (CESA-2020:1190)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012518.html>**BDU:2019-04730 (FSTEC)**<https://bdu.fstec.ru/vul/2019-04730>**CVE-2018-14567 (CVE)**

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 4.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L)

CWE-835

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14567>

RHSA-2020:1190 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:1190>

Уязвимость	Риск: Средний
ALTX ID 320104	Red Hat/CentOS -- уязвимость в evolution-data-server, evolution, atk, evolution-ews (CVE-2018-15587)
Описание	

В продукте evolution-data-server, evolution, atk, evolution-ews обнаружена уязвимость CVE-2018-15587.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129152

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129152>

CESA-2020:1080-CentOS 7 (CESA-2020:1080)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012408.html>

RHSA-2020:1600 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1600>

BDU:2019-02900 (FSTEC)

<https://bdu.fstec.ru/vul/2019-02900>

CVE-2018-15587 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)

CWE-347

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15587>

RHSA-2020:1080 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1080>

Уязвимость	Риск: Средний
ALTX ID 320110	Red Hat/CentOS -- уязвимость в httpd, httpd:2.4 (CVE-2018-17199)
Описание	

В продуктах httpd, httpd:2.4 обнаружена уязвимость CVE-2018-17199.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129158

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129158>

CESA-2020:1121 (CESA-2020:1121)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012463.html>

RHSA-2021:1809 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1809>

BDU:2019-01564 (FSTEC)

<https://bdu.fstec.ru/vul/2019-01564>

CVE-2018-17199 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
 CVSSv3: Базовая оценка 5.4 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)
 CWE-384
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17199>

RHSA-2020:1121 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1121>

Уязвимость	Риск: Средний
ALTX ID 320118	Red Hat/CentOS -- уязвимость в python3, Python, python27 (CVE-2018-20852)

Описание

В продуктах python3, Python, python27 обнаружена уязвимость CVE-2018-20852.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

- oval:ru.altx-soft.nix:def:129166**
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129166>
- CESA-2020:1132 (CESA-2020:1132)**
<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012572.html>
- CESA-2020:1131 (CESA-2020:1131)**
<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012571.html>
- BDU:2021-00373 (FSTEC)**
<https://bdu.fstec.ru/vul/2021-00373>
- RHSA-2020:1764 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:1764>
- RHSA-2020:1605 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:1605>
- CVE-2018-20852 (CVE)**
 CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
 CVSSv3: Базовая оценка 5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
 CWE-20
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20852>
- RHSA-2020:1132 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:1132>
- RHSA-2020:1131 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:1131>

Уязвимость	Риск: Средний
ALTX ID 320120	Red Hat/CentOS -- уязвимость в cups (CVE-2018-4180)

Описание

В продукте cups обнаружена уязвимость CVE-2018-4180.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129168

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129168>

CESA-2020:1050 (CESA-2020:1050)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012427.html>

BDU:2019-01630 (FSTEC)

<https://bdu.fstec.ru/vul/2019-01630>

CVE-2018-4180 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 6.6 (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4180>

RHSA-2020:1050 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1050>

Уязвимость

Риск: Средний

ALTX ID

320121

Red Hat/CentOS -- уязвимость в cups (CVE-2018-4181)

Описание

В продукте cups обнаружена уязвимость CVE-2018-4181.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129169

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129169>

CESA-2020:1050 (CESA-2020:1050)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012427.html>

BDU:2019-01632 (FSTEC)

<https://bdu.fstec.ru/vul/2019-01632>

CVE-2018-4181 (CVE)

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:C/I:N/A:N)

CVSSv3: Базовая оценка 5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4181>

RHSA-2020:1050 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1050>

Уязвимость

Риск: Средний

ALTX ID

320122

Red Hat/CentOS -- уязвимость в cups (CVE-2018-4700)

Описание

В продукте cups обнаружена уязвимость CVE-2018-4700.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129170

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129170>

CESA-2020:1050 (CESA-2020:1050)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012427.html>

CVE-2018-4700 (CVE)

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4700>

RHSA-2020:1050 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1050>

Уязвимость

Риск: Средний

ALTX ID

320123

Red Hat/CentOS -- уязвимость в php (CVE-2018-5712)

Описание

В продукте php обнаружена уязвимость CVE-2018-5712.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129171

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129171>

CESA-2020:1112 (CESA-2020:1112)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012562.html>

BDU:2019-04386 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04386>

CVE-2018-5712 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 6.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CWE-79

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5712>

RHSA-2020:1112 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1112>

Уязвимость

Риск: Средний

ALTX ID

320124

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2018-7191)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2018-7191.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129172

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129172>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

RHSA-2020:2522 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2522>

RHSA-2020:2851 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2851>

BDU:2020-02562 (FSTEC)<https://bdu.fstec.ru/vul/2020-02562>**CVE-2018-7191 (CVE)**

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 6.1 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7191>**RHSA-2020:1070 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1070>**RHSA-2020:1016 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1016>

Уязвимость

Риск: Средний

ALTX ID

320126

Red Hat/CentOS -- уязвимость в php (CVE-2018-7584)**Описание**

В продукте php обнаружена уязвимость CVE-2018-7584.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:129174**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129174>**CESA-2020:1112 (CESA-2020:1112)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012562.html>**44846 (EXPLOIT-DB)**<https://www.exploit-db.com/exploits/44846>**BDU:2018-00525 (FSTEC)**<https://bdu.fstec.ru/vul/2018-00525>**CVE-2018-7584 (CVE)**

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-119

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7584>**RHSA-2020:1112 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1112>

Уязвимость

Риск: Средний

ALTX ID

320139

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-12382)**Описание**

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-12382.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:129187**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129187>

BDU:2021-06329 (FSTEC)<https://bdu.fstec.ru/vul/2021-06329>**CESA-2020:1016 (CESA-2020:1016)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>**RHSA-2020:2522 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:2522>**CVE-2019-12382 (CVE)**

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12382>**RHSA-2020:1070 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1070>**RHSA-2020:1016 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1016>

Уязвимость

Риск: Средний

ALTX ID
320163**Red Hat/CentOS -- уязвимость в kernel, bpftool (CVE-2019-13648)**

Описание

В продуктах kernel, bpftool обнаружена уязвимость CVE-2019-13648.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129211<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129211>**CESA-2020:1016 (CESA-2020:1016)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>**RHSA-2020:3019 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3019>**BDU:2019-03627 (FSTEC)**<https://bdu.fstec.ru/vul/2019-03627>**CVE-2019-13648 (CVE)**

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-399

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13648>**RHSA-2020:1016 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1016>

Уязвимость

Риск: Средний

ALTX ID
320164**Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-14283)**

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-14283.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129212

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129212>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

RHSA-2020:2522 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2522>

BDU:2019-03410 (FSTEC)

<https://bdu.fstec.ru/vul/2019-03410>

CVE-2019-14283 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 5.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:H)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14283>

RHSA-2020:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1070>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

Уязвимость

Риск: Средний

ALTX ID

320172

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-15221)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-15221.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129220

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129220>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

RHSA-2020:1567 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1567>

RHSA-2020:1769 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1769>

BDU:2019-03087 (FSTEC)

<https://bdu.fstec.ru/vul/2019-03087>

CVE-2019-15221 (CVE)

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 4.5 (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15221>

RHSA-2020:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1070>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

Уязвимость

Риск: Средний

ALTX ID

320173

Red Hat/CentOS -- уязвимость в python3, Python, python27 (CVE-2019-16056)

Описание

В продуктах python3, Python, python27 обнаружена уязвимость CVE-2019-16056.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129221

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129221>

CESA-2020:1132 (CESA-2020:1132)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012572.html>

CESA-2020:1131 (CESA-2020:1131)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012571.html>

RHSA-2020:2520 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2520>

RHSA-2020:1764 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1764>

RHSA-2020:1605 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1605>

BDU:2020-01347 (FSTEC)

<https://bdu.fstec.ru/vul/2020-01347>

CVE-2019-16056 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 7.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16056>

RHSA-2020:1132 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1132>

RHSA-2020:1131 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1131>

Уязвимость

Риск: Средний

ALTX ID

320181

Red Hat/CentOS -- уязвимость в Rsyslog (CVE-2019-17041)

Описание

В продукте Rsyslog обнаружена уязвимость CVE-2019-17041.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129229

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129229>

CESA-2020:1000 (CESA-2020:1000)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012594.html>

RHSA-2020:1702 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1702>

VULN-20200401.2 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20200401.2.pdf>

BDU:2020-01363 (FSTEC)

<https://bdu.fstec.ru/vul/2020-01363>

CVE-2019-17041 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17041>

RHSA-2020:1000 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1000>

Уязвимость	Риск: Средний
ALT X ID 320182	Red Hat/CentOS -- уязвимость в Rsyslog (CVE-2019-17042)
Описание	

В продукте Rsyslog обнаружена уязвимость CVE-2019-17042.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129230

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129230>

CESA-2020:1000 (CESA-2020:1000)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012594.html>

BDU:2021-01479 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01479>

RHSA-2020:1702 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1702>

VULN-20200401.2 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20200401.2.pdf>

CVE-2019-17042 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-20

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17042>

RHSA-2020:1000 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1000>

Уязвимость	Риск: Средний
ALT X ID 320186	Red Hat/CentOS -- уязвимость в kernel (CVE-2019-18660)
Описание	

В продукте kernel обнаружена уязвимость CVE-2019-18660.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129234

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129234>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

RHSA-2020:1984 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1984>

RHSA-2020:2851 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2851>

RHSA-2020:2933 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2933>

BDU:2020-02944 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02944>

RHSA-2020:1372 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1372>

CVE-2019-18660 (CVE)

CVSSv2: Базовая оценка 1.8 (AV:L/AC:M/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 4.6 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)

CWE-200

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18660>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

Уязвимость	Риск: Средний
ALTX ID 320189	Red Hat/CentOS -- уязвимость в gnome (CVE-2019-3820)
Описание	

В продукте gnome обнаружена уязвимость CVE-2019-3820.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129237

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129237>

CESA-2020:1021-CentOS 7 (CESA-2020:1021)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012403.html>

CVE-2019-3820 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 4.8 (CVSS:3.0/AV:P/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L)

CWE-287

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-3820>

RHSA-2020:1021 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1021>

Уязвимость	Риск: Средний
ALTX ID 320190	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-3901)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-3901.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129238

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129238>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

RHSA-2020:2522 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2522>

RHSA-2020:2851 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2851>

CVE-2019-3901 (CVE)

CVSSv2: Базовая оценка 1.8 (AV:L/AC:M/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 5.5 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N)

CWE-667

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-3901>

RHSA-2020:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1070>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

Уязвимость

Риск: Средний

ALT X ID

320191

Red Hat/CentOS -- уязвимость в curl, Libcurl (CVE-2019-5436)

Описание

В продуктах curl, Libcurl обнаружена уязвимость CVE-2019-5436.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129239

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129239>

CESA-2020:1020 (CESA-2020:1020)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012428.html>

RHSA-2020:2505 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2505>

RHSA-2020:1792 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1792>

VULN-20200401.3 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20200401.3.pdf>

BDU:2019-03793 (FSTEC)

<https://bdu.fstec.ru/vul/2019-03793>

BDU:2019-02099 (FSTEC)

<https://bdu.fstec.ru/vul/2019-02099>

CVE-2019-5436 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5436>

RHSA-2020:1020 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1020>

Уязвимость

Риск: Средний

ALTX ID

320192

Red Hat/CentOS -- уязвимость в Bind (CVE-2019-6477)

Описание

В продукте Bind обнаружена уязвимость CVE-2019-6477.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129240

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129240>

CESA-2020:1061 (CESA-2020:1061)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012415.html>

RHSA-2020:1845 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1845>

BDU:2019-04891 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04891>

CVE-2019-6477 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-400

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6477>

RHSA-2020:1061 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1061>

Уязвимость

Риск: Средний

ALTX ID

320196

Red Hat/CentOS -- уязвимость в dovecot (CVE-2019-7524)

Описание

В продукте dovecot обнаружена уязвимость CVE-2019-7524.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129244

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129244>

CESA-2020:1062 (CESA-2020:1062)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012433.html>

BDU:2019-01562 (FSTEC)

<https://bdu.fstec.ru/vul/2019-01562>

CVE-2019-7524 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 6.5 (CVSS:3.0/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H)

CWE-119

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7524>

RHSA-2020:1062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1062>

Уязвимость

Риск: Средний

ALTX ID

320197

Red Hat/CentOS -- уязвимость в php (CVE-2019-9024)

Описание

В продукте php обнаружена уязвимость CVE-2019-9024.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129245

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129245>

CESA-2020:1112 (CESA-2020:1112)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012562.html>

RHSA-2020:1624 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1624>

BDU:2019-01555 (FSTEC)

<https://bdu.fstec.ru/vul/2019-01555>

CVE-2019-9024 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9024>

RHSA-2020:1112 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1112>

Уязвимость

Риск: Средний

ALTX ID

320206

Red Hat/CentOS -- уязвимость в bash (CVE-2019-9924)

Описание

В продукте bash обнаружена уязвимость CVE-2019-9924.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129254

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129254>

RHSA-2020:3592 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3592>

VULN-20211206.4 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20211206.4.pdf>

CESA-2020:1113 (CESA-2020:1113)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012412.html>

RHSA-2020:3803 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3803>

RHSA-2020:3474 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3474>

BDU:2019-01405 (FSTEC)

<https://bdu.fstec.ru/vul/2019-01405>

CVE-2019-9924 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
 CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
 CWE-862
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9924>

RHSA-2020:1113 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1113>

Уязвимость	Риск: Средний
ALTX ID 321554	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19527)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19527.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129495
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129495>

RHSA-2020:4236 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:4236>

CESA-2020:3220 (CESA-2020:3220)
<http://lists.centos.org/pipermail/centos-announce/2020-July/035780.html>

RHSA-2020:3220 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:3220>

RHSA-2020:3221 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:3221>

RHSA-2020:1372 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:1372>

BDU:2020-00295 (FSTEC)
<https://bdu.fstec.ru/vul/2020-00295>

CVE-2019-19527 (CVE)
 CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
 CVSSv3: Базовая оценка 6.8 (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
 CWE-416
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19527>

RHSA-2020:1378 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:1378>

Уязвимость	Риск: Средний
ALTX ID 323683	Red Hat/CentOS -- уязвимость в glib2, ibus (CVE-2019-14822)
Описание	

В продуктах glib2, ibus обнаружена уязвимость CVE-2019-14822.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:130803

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:130803>

RHSA-2020:3978 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3978>

CESA-2020:3978-CentOS 7 (CESA-2020:3978)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012712.html>

BDU:2020-02043 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02043>

CVE-2019-14822 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:P/I:P/A:N)

CVSSv3: Базовая оценка 6.0 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N)

CWE-862

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14822>

RHSA-2020:1880 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1880>

Уязвимость

Риск: Средний

ALTX ID
323693

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19534)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19534.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:130813

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:130813>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

BDU:2020-00296 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00296>

CVE-2019-19534 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 4.5 (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CWE-909

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19534>

RHSA-2020:1567 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1567>

RHSA-2020:1769 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1769>

Уязвимость

Риск: Средний

ALTX ID
323700

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-1749)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-1749.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:130820

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:130820>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

BDU:2020-01065 (FSTEC)

<https://bdu.fstec.ru/vul/2020-01065>

CVE-2020-1749 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

CWE-319

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1749>

RHSA-2020:1567 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1567>

RHSA-2020:1769 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1769>

Уязвимость

Риск: Средний

ALTX ID

324169

Red Hat/CentOS -- уязвимость в e2fsprogs (CVE-2019-5094)

Описание

В продукте e2fsprogs обнаружена уязвимость CVE-2019-5094.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:131204

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:131204>

VULN-20220727.2 (НККИ)

<https://safe-surf.ru/upload/VULN/VULN-20220727.2.pdf>

CESA-2020:4011 (CESA-2020:4011)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012685.html>

RHSA-2020:4011 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4011>

BDU:2019-04671 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04671>

CVE-2019-5094 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 6.4 (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5094>

RHSA-2020:1913 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1913>

Уязвимость

Риск: Средний

ALTX ID
324171

Red Hat/CentOS -- уязвимость в curl (CVE-2019-5482)

Описание

В продукте curl обнаружена уязвимость CVE-2019-5482.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:131206

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:131206>

RHSA-2021:1027 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1027>

RHSA-2021:0877 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0877>

RHSA-2021:0759 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0759>

CESA-2020:3916 (CESA-2020:3916)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012676.html>

RHSA-2020:3916 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3916>

BDU:2019-04539 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04539>

CVE-2019-5482 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 6.3 (CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5482>

RHSA-2020:1792 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1792>

Уязвимость

Риск: Средний

ALTX ID
324776

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-2732)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-2732.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:131443

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:131443>

BDU:2020-05885 (FSTEC)

<https://bdu.fstec.ru/vul/2020-05885>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

CVE-2020-2732 (CVE)

CVSSv2: Базовая оценка 2.2 (AV:A/AC:M/Au:S/C:P/I:N/A:N)

CVSSv3: Базовая оценка 5.8 (CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N)

CWE-200

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2732>

RHSA-2020:2102 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2102>

RHSA-2020:2171 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2171>

Уязвимость	Риск: Средний
ALTX ID 326423	Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-0543)
Описание	

В продукте microcode_ctl обнаружена уязвимость CVE-2020-0543.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:132631

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:132631>

RHSA-2021:3364 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3364>

RHSA-2021:3322 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3322>

RHSA-2021:3317 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3317>

RHSA-2021:3323 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3323>

RHSA-2021:3176 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3176>

RHSA-2021:3255 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3255>

RHSA-2021:3028 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3028>

CESA-2021:3028 (CESA-2021:3028)

<http://lists.centos.org/pipermail/centos-announce/2021-August/048347.html>

RHSA-2021:3029 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3029>

RHSA-2021:3027 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3027>

CESA-2020:2433 (CESA-2020:2433)

<http://lists.centos.org/pipermail/centos-announce/2020-June/035752.html>

RHSA-2020:2842 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2842>

RHSA-2020:2432 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2432>

CESA-2020:2432 (CESA-2020:2432)

<http://lists.centos.org/pipermail/centos-announce/2020-June/035754.html>

BDU:2020-04459 (FSTEC)

<https://bdu.fstec.ru/vul/2020-04459>

RHSA-2020:2758 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2758>

RHSA-2020:2771 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2771>

RHSA-2020:2677 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2677>

RHSA-2020:2679 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2679>

RHSA-2020:2680 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2680>

RHSA-2020:2706 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2706>

RHSA-2020:2707 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2707>

CVE-2020-0543 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)

CWE-459

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0543>

RHSA-2020:2433 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2433>

RHSA-2020:2431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2431>

Уязвимость	Риск: Средний
ALTX ID 326425	Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-0549)

Описание

В продукте microcode_ctl обнаружена уязвимость CVE-2020-0549.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:132633

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:132633>

RHSA-2021:3364 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3364>

RHSA-2021:3322 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3322>

RHSA-2021:3317 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3317>

RHSA-2021:3323 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3323>

RHSA-2021:3176 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3176>

RHSA-2021:3255 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3255>

RHSA-2021:3028 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3028>

CESA-2021:3028 (CESA-2021:3028)

<http://lists.centos.org/pipermail/centos-announce/2021-August/048347.html>

RHSA-2021:3029 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3029>

RHSA-2021:3027 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3027>

CESA-2020:2433 (CESA-2020:2433)

<http://lists.centos.org/pipermail/centos-announce/2020-June/035752.html>

RHSA-2020:2842 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2842>

RHSA-2020:2432 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2432>

CESA-2020:2432 (CESA-2020:2432)

<http://lists.centos.org/pipermail/centos-announce/2020-June/035754.html>

RHSA-2020:2758 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2758>

RHSA-2020:2771 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2771>

RHSA-2020:2677 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2677>

RHSA-2020:2679 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2679>

RHSA-2020:2680 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2680>

RHSA-2020:2706 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2706>

RHSA-2020:2707 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2707>

BDU:2020-00307 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00307>

CVE-2020-0549 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 6.5 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)

CWE-404

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0549>

RHSA-2020:2433 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2433>

RHSA-2020:2431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2431>

Уязвимость	Риск: Средний
ALTX ID 327659	Red Hat/CentOS -- уязвимость в kernel, kernel-rt, kernel-rt-debug, kernel-rt-debug-devel, kernel-rt-devel, kernel-rt-doc, kernel-rt-trace, kernel-rt-trace-devel, bpftool (CVE-2020-12888)
Описание	В продукте kernel, kernel-rt, kernel-rt-debug, kernel-rt-debug-devel, kernel-rt-devel, kernel-rt-doc, kernel-rt-trace, kernel-rt-trace-devel, bpftool обнаружена уязвимость CVE-2020-12888.
Исправление	Необходимо установить актуальное обновление от производителя.
Ссылки	

oval:ru.altx-soft.nix:def:133119

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:133119>

RHSA-2020:3041 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3041>

CESA-2020:2664 (CESA-2020:2664)

<http://lists.centos.org/pipermail/centos-announce/2020-June/035769.html>

BDU:2021-00471 (FSTEC)

<https://bdu.fstec.ru/vul/2021-00471>

RHSA-2020:3222 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3222>

RHSA-2020:3010 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3010>

RHSA-2020:3230 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3230>

RHSA-2020:2831 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2831>

RHSA-2020:2832 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2832>

RHSA-2020:2851 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2851>

RHSA-2020:3016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3016>

RHSA-2020:3019 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3019>

CVE-2020-12888 (CVE)

CVSSv2: Базовая оценка 4.6 (AV:L/AC:M/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H)

CWE-755

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12888>

RHSA-2020:2664 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2664>

RHSA-2020:2665 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2665>

Уязвимость	Риск: Средний
ALTX ID 329835	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-12653)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-12653.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:135080

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:135080>

RHSA-2020:3041 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3041>

CESA-2020:3220 (CESA-2020:3220)

<http://lists.centos.org/pipermail/centos-announce/2020-July/035780.html>

RHSA-2020:3432 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3432>

VULN-20200803.3 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20200803.3.pdf>

RHSA-2020:3232 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3232>

RHSA-2020:3222 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3222>

RHSA-2020:3010 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3010>

RHSA-2020:3220 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3220>

RHSA-2020:3221 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3221>

RHSA-2020:3226 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3226>

RHSA-2020:3224 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3224>

RHSA-2020:3016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3016>

BDU:2020-03360 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03360>

CVE-2020-12653 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12653>

RHSA-2020:2832 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2832>

Уязвимость	Риск: Средний
ALT X ID 329836	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-12654)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-12654.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:135081

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:135081>

RHSA-2020:3041 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3041>

CESA-2020:3220 (CESA-2020:3220)

<http://lists.centos.org/pipermail/centos-announce/2020-July/035780.html>

RHSA-2020:3432 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3432>

VULN-20200803.3 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20200803.3.pdf>

RHSA-2020:3232 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3232>

RHSA-2020:3222 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3222>

RHSA-2020:3010 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3010>

RHSA-2020:3220 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3220>

RHSA-2020:3221 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3221>

RHSA-2020:3226 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3226>

RHSA-2020:3224 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3224>

RHSA-2020:3016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3016>

BDU:2020-03361 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03361>

CVE-2020-12654 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:A/AC:H/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12654>

RHSA-2020:2832 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2832>

Уязвимость	Риск: Средний
ALTX ID 330685	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10757)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-10757.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:135394

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:135394>

RHSA-2020:3041 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3041>

BDU:2021-06410 (FSTEC)

<https://bdu.fstec.ru/vul/2021-06410>

CESA-2020:3220 (CESA-2020:3220)

<http://lists.centos.org/pipermail/centos-announce/2020-July/035780.html>

RHSA-2020:3598 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3598>

VULN-20200803.3 (NKCKI)

<http://safe-surf.ru/upload/VULN/VULN-20200803.3.pdf>

RHSA-2020:3222 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3222>

RHSA-2020:3010 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3010>

RHSA-2020:3220 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3220>

RHSA-2020:3221 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3221>

RHSA-2020:3226 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3226>

CVE-2020-10757 (CVE)

CVSSv2: Базовая оценка 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-119

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10757>

RHSA-2020:3016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3016>

Уязвимость	Риск: Средний
ALTX ID 330691	Red Hat/CentOS -- уязвимость в dbus (CVE-2020-12049)
Описание	

В продукте dbus обнаружена уязвимость CVE-2020-12049.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:135400

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:135400>

RHSA-2020:3044 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3044>

BDU:2021-03403 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03403>

CESA-2020:2894 (CESA-2020:2894)

<http://lists.centos.org/pipermail/centos-announce/2020-July/035777.html>

RHSA-2020:3298 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3298>

RHSA-2020:3014 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3014>

CVE-2020-12049 (CVE)

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H)

CWE-404

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12049>

RHSA-2020:2894 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2894>

Уязвимость	Риск: Средний
ALTX ID 332428	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-14308)
Описание	

В продуктах grub2, shim, fwupd обнаружена уязвимость CVE-2020-14308.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:137029

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:137029>

RHSA-2020:3227 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3227>

CESA-2020:3217-CentOS 7 (CESA-2020:3217)

<http://lists.centos.org/pipermail/centos-announce/2020-July/035781.html>

RHSA-2020:3274 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3274>

RHSA-2020:3275 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3275>

BDU:2020-03955 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03955>

RHSA-2020:3271 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3271>

RHSA-2020:3273 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3273>

RHSA-2020:3276 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3276>

CVE-2020-14308 (CVE)

CVSSv2: Базовая оценка 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 6.4 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14308>

RHSA-2020:3216 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3216>

RHSA-2020:3217 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3217>

RHSA-2020:3223 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3223>

Уязвимость	Риск: Средний
ALTX ID 332429	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-14309)
Описание	

В продуктах grub2, shim, fwupd обнаружена уязвимость CVE-2020-14309.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:137030

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:137030>

RHSA-2020:3227 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3227>

CESA-2020:3217-CentOS 7 (CESA-2020:3217)

<http://lists.centos.org/pipermail/centos-announce/2020-July/035781.html>

RHSA-2020:3274 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3274>

RHSA-2020:3275 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3275>

BDU:2020-03968 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03968>

RHSA-2020:3271 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3271>

RHSA-2020:3273 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3273>

RHSA-2020:3276 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3276>

CVE-2020-14309 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 6.6 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14309>

RHSA-2020:3216 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3216>

RHSA-2020:3217 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3217>

RHSA-2020:3223 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3223>

Уязвимость	Риск: Средний
ALT X ID 332430	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-14310)
Описание	

В продуктах grub2, shim, fwupd обнаружена уязвимость CVE-2020-14310.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:137031

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:137031>

RHSA-2020:3227 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3227>

CESA-2020:3217-CentOS 7 (CESA-2020:3217)

<http://lists.centos.org/pipermail/centos-announce/2020-July/035781.html>

RHSA-2020:3274 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3274>

RHSA-2020:3275 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3275>

BDU:2020-03969 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03969>

RHSA-2020:3271 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3271>

RHSA-2020:3273 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3273>

RHSA-2020:3276 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3276>

CVE-2020-14310 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:N/I:P/A:P)

CVSSv3: Базовая оценка 5.6 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14310>

RHSA-2020:3216 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3216>

RHSA-2020:3217 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:3217>**RHSA-2020:3223 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3223>

Уязвимость	Риск: Средний
ALTX ID 332431	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-14311)

Описание

В продуктах grub2, shim, fwupd обнаружена уязвимость CVE-2020-14311.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:137032

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:137032>

RHSA-2020:3227 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3227>

CESA-2020:3217-CentOS 7 (CESA-2020:3217)

<http://lists.centos.org/pipermail/centos-announce/2020-July/035781.html>

RHSA-2020:3274 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3274>

RHSA-2020:3275 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3275>

BDU:2020-03970 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03970>

RHSA-2020:3271 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3271>

RHSA-2020:3273 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3273>

RHSA-2020:3276 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3276>

CVE-2020-14311 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:N/I:P/A:P)

CVSSv3: Базовая оценка 5.6 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14311>

RHSA-2020:3216 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3216>

RHSA-2020:3217 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3217>

RHSA-2020:3223 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3223>

Уязвимость	Риск: Средний
ALTX ID 332434	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-15705)

Описание

В продуктах grub2, shim, fwupd обнаружена уязвимость CVE-2020-15705.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:137035

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:137035>

RHSA-2020:3227 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3227>

BDU:2022-05895 (FSTEC)

<https://bdu.fstec.ru/vul/2022-05895>

CESA-2020:3217-CentOS 7 (CESA-2020:3217)

<http://lists.centos.org/pipermail/centos-announce/2020-July/035781.html>

RHSA-2020:3274 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3274>

RHSA-2020:3275 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3275>

RHSA-2020:3271 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3271>

RHSA-2020:3273 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3273>

RHSA-2020:3276 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3276>

CVE-2020-15705 (CVE)

CVSSv2: Базовая оценка 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 6.4 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)

CWE-347

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15705>

RHSA-2020:3216 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3216>

RHSA-2020:3217 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3217>

RHSA-2020:3223 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3223>

Уязвимость

Риск: Средний

ALTX ID

332435

Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-15706)

Описание

В продуктах grub2, shim, fwupd обнаружена уязвимость CVE-2020-15706.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:137036

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:137036>

RHSA-2020:3227 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3227>

CESA-2020:3217-CentOS 7 (CESA-2020:3217)

<http://lists.centos.org/pipermail/centos-announce/2020-July/035781.html>

RHSA-2020:3274 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3274>

RHSA-2020:3275 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3275>

BDU:2020-03971 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03971>

RHSA-2020:3271 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3271>

RHSA-2020:3273 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3273>

RHSA-2020:3276 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3276>

CVE-2020-15706 (CVE)

CVSSv2: Базовая оценка 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 6.4 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)

CWE-362

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15706>

RHSA-2020:3216 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3216>

RHSA-2020:3217 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3217>

RHSA-2020:3223 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3223>

Уязвимость

Риск: Средний

ALTX ID 332436	Red Hat/CentOS -- уязвимость в grub2, shim, fwupd (CVE-2020-15707)
-------------------	---

Описание

В продуктах grub2, shim, fwupd обнаружена уязвимость CVE-2020-15707.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:137037

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:137037>

RHSA-2020:3227 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3227>

CESA-2020:3217-CentOS 7 (CESA-2020:3217)

<http://lists.centos.org/pipermail/centos-announce/2020-July/035781.html>

RHSA-2020:3274 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3274>

RHSA-2020:3275 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3275>

BDU:2020-03972 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03972>

RHSA-2020:3271 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3271>

RHSA-2020:3276 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3276>

CVE-2020-15707 (CVE)

CVSSv2: Базовая оценка 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 5.6 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H)

CWE-362

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15707>

RHSA-2020:3216 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:3216>**RHSA-2020:3217 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3217>**RHSA-2020:3223 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3223>

Уязвимость

Риск: Средний

ALTX ID
333902**Red Hat/CentOS -- уязвимость в nspr, nss, nss-softokn (CVE-2019-11756)****Описание**

В продуктах nspr, nss, nss-softokn обнаружена уязвимость CVE-2019-11756.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:138452**<https://ovaldbrn.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:138452>**CESA-2020:4076-CentOS 7 (CESA-2020:4076)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-November/012876.html>**RHSA-2021:1026 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:1026>**RHSA-2021:0876 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0876>**RHSA-2021:0758 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0758>**RHSA-2020:4076 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4076>**BDU:2020-01795 (FSTEC)**<https://bdu.fstec.ru/vul/2020-01795>**CVE-2019-11756 (CVE)**

CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.0 (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11756>**RHSA-2020:3280 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3280>

Уязвимость

Риск: Средний

ALTX ID
333904**Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2019-17023)****Описание**

В продуктах nspr, nss обнаружена уязвимость CVE-2019-17023.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:138454**

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:138454>

CESA-2020:4076-CentOS 7 (CESA-2020:4076)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-November/012876.html>

RHSA-2020:4076 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4076>

BDU:2020-01970 (FSTEC)

<https://bdu.fstec.ru/vul/2020-01970>

CVE-2019-17023 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N)

CWE-287

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17023>

RHSA-2020:3280 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3280>

Уязвимость

Риск: Средний

ALT X ID

335564

Red Hat/CentOS -- уязвимость в dovecot (CVE-2020-12100)

Описание

В продукте dovecot обнаружена уязвимость CVE-2020-12100.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:139387

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:139387>

RHSA-2020:3735 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3735>

BDU:2020-05783 (FSTEC)

<https://bdu.fstec.ru/vul/2020-05783>

CESA-2020:3617 (CESA-2020:3617)

<http://lists.centos.org/pipermail/centos-announce/2020-September/035809.html>

RHSA-2020:3736 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3736>

RHSA-2020:3713 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3713>

CVE-2020-12100 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-674

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12100>

RHSA-2020:3617 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3617>

Уязвимость

Риск: Средний

ALT X ID

335565

Red Hat/CentOS -- уязвимость в dovecot (CVE-2020-12673)

Описание

В продукте dovecot обнаружена уязвимость CVE-2020-12673.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:139388

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:139388>

RHSA-2020:3735 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3735>

BDU:2020-05789 (FSTEC)

<https://bdu.fstec.ru/vul/2020-05789>

CESA-2020:3617 (CESA-2020:3617)

<http://lists.centos.org/pipermail/centos-announce/2020-September/035809.html>

RHSA-2020:3736 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3736>

RHSA-2020:3713 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3713>

CVE-2020-12673 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12673>

RHSA-2020:3617 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3617>

Уязвимость

Риск: Средний

ALTX ID

335566

Red Hat/CentOS -- уязвимость в dovecot (CVE-2020-12674)

Описание

В продукте dovecot обнаружена уязвимость CVE-2020-12674.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:139389

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:139389>

RHSA-2020:3735 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3735>

BDU:2020-05782 (FSTEC)

<https://bdu.fstec.ru/vul/2020-05782>

CESA-2020:3617 (CESA-2020:3617)

<http://lists.centos.org/pipermail/centos-announce/2020-September/035809.html>

RHSA-2020:3736 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3736>

RHSA-2020:3713 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3713>

CVE-2020-12674 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12674>

RHSA-2020:3617 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:3617>

Уязвимость

Риск: Средний

ALTX ID
336285**Red Hat/CentOS -- уязвимость в libcroco (CVE-2020-12825)****Описание**

В продукте libcroco обнаружена уязвимость CVE-2020-12825.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:139617**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:139617>**CESA-2020:4072 (CESA-2020:4072)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-November/012873.html>**RHSA-2020:4072 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4072>**CVE-2020-12825 (CVE)**

CVSSv2: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:N/I:P/A:P)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H)

CWE-674

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12825>**RHSA-2020:3654 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3654>

Уязвимость

Риск: Средний

ALTX ID
336583**Red Hat/CentOS -- уязвимость в mysql:8.0, mariadb:10.3, mariadb, MySQL (CVE-2019-2974)****Описание**

В продукте mysql:8.0, mariadb:10.3, mariadb, MySQL обнаружена уязвимость CVE-2019-2974.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:139823**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:139823>**RHSA-2020:3755 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:3755>**RHSA-2020:5663 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5663>**BDU:2019-03900 (FSTEC)**<https://bdu.fstec.ru/vul/2019-03900>**RHSA-2020:5665 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5665>**RHSA-2020:5654 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5654>

RHSA-2020:5500 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5500>

CESA-2020:4026 (CESA-2020:4026)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012775.html>

RHSA-2020:4026 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4026>

CVE-2019-2974 (CVE)

CVSSv2: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)

CVSSv3: Базовая оценка 6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-2974>

RHSA-2020:3757 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3757>

RHSA-2020:3732 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3732>

Уязвимость	Риск: Средний
ALTX ID 336629	Red Hat/CentOS -- уязвимость в mysql:8.0, mariadb-connector-c, mariadb:10.3, mariadb, MySQL (CVE-2020-2574)
Описание	

В продукте mysql:8.0, mariadb-connector-c, mariadb:10.3, mariadb, MySQL обнаружена уязвимость CVE-2020-2574.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:139869

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:139869>

RHSA-2020:3755 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3755>

RHSA-2020:5662 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5662>

RHSA-2020:5663 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5663>

RHSA-2020:5665 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5665>

RHSA-2020:5660 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5660>

RHSA-2020:5655 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5655>

RHSA-2020:5654 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5654>

RHSA-2020:5503 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5503>

RHSA-2020:5500 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5500>

CESA-2020:4026 (CESA-2020:4026)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012775.html>

RHSA-2020:4026 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4026>

BDU:2020-00431 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00431>

CVE-2020-2574 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
 CVSSv3: Базовая оценка 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
 NVD-CWE-noinfo
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2574>

RHSA-2020:3757 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3757>

RHSA-2020:3732 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3732>

Уязвимость	Риск: Средний
ALT X ID 336641	Red Hat/CentOS -- уязвимость в mysql:8.0, mariadb-connector-c, mariadb:10.3, mariadb, MySQL (CVE-2020-2752)
Описание	

В продукте mysql:8.0, mariadb-connector-c, mariadb:10.3, mariadb, MySQL обнаружена уязвимость CVE-2020-2752.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

- oval:ru.altx-soft.nix:def:139881**
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:139881>
- RHSA-2020:3755 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:3755>
- RHSA-2020:5662 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:5662>
- RHSA-2020:5663 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:5663>
- RHSA-2020:5665 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:5665>
- RHSA-2020:5660 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:5660>
- RHSA-2020:5655 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:5655>
- RHSA-2020:5654 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:5654>
- RHSA-2020:5503 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:5503>
- RHSA-2020:5500 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:5500>
- CESA-2020:4026 (CESA-2020:4026)**
<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012775.html>
- RHSA-2020:4026 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:4026>
- BDU:2020-02644 (FSTEC)**
<https://bdu.fstec.ru/vul/2020-02644>
- CVE-2020-2752 (CVE)**
 CVSSv2: Базовая оценка 3.5 (AV:N/AC:M/Au:S/C:N/I:N/A:P)
 CVSSv3: Базовая оценка 5.3 (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)
 NVD-CWE-noinfo
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2752>
- RHSA-2020:3757 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:3757>

RHSA-2020:3732 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:3732>

Уязвимость	Риск: Средний
ALTX ID 336651	Red Hat/CentOS -- уязвимость в mysql:8.0, mariadb:10.3, mariadb, MySQL (CVE-2020-2780)
Описание	

В продукте mysql:8.0, mariadb:10.3, mariadb, MySQL обнаружена уязвимость CVE-2020-2780.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:139891

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:139891>

RHSA-2020:3755 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3755>

RHSA-2020:5663 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5663>

RHSA-2020:5665 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5665>

RHSA-2020:5654 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5654>

RHSA-2020:5500 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5500>

CESA-2020:4026 (CESA-2020:4026)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012775.html>

RHSA-2020:4026 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4026>

BDU:2020-02647 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02647>

CVE-2020-2780 (CVE)

CVSSv2: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)

CVSSv3: Базовая оценка 6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2780>

RHSA-2020:3757 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3757>

RHSA-2020:3732 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3732>

Уязвимость	Риск: Средний
ALTX ID 336653	Red Hat/CentOS -- уязвимость в mysql:8.0, mariadb:10.3, mariadb, MySQL (CVE-2020-2812)
Описание	

В продукте mysql:8.0, mariadb:10.3, mariadb, MySQL обнаружена уязвимость CVE-2020-2812.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:139893

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:139893>

RHSA-2020:3755 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3755>

RHSA-2020:5663 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5663>

RHSA-2020:5665 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5665>

RHSA-2020:5654 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5654>

RHSA-2020:5500 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5500>

CESA-2020:4026 (CESA-2020:4026)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012775.html>

RHSA-2020:4026 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4026>

BDU:2020-02648 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02648>

CVE-2020-2812 (CVE)

CVSSv2: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)

CVSSv3: Базовая оценка 4.9 (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2812>

RHSA-2020:3757 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3757>

RHSA-2020:3732 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3732>

Уязвимость

Риск: Средний

ALTX ID
337335

Red Hat/CentOS -- уязвимость в kernel (CVE-2017-18551)

Описание

В продукте kernel обнаружена уязвимость CVE-2017-18551.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140467

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140467>

RHSA-2020:5656 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5656>

RHSA-2020:5430 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5430>

RHSA-2020:5206 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5206>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2017-18551 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)
 CVSSv3: Базовая оценка 6.6 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)
 CWE-787
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18551>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость	Риск: Средний
ALTX ID 337336	Red Hat/CentOS -- уязвимость в kernel (CVE-2018-20836)
Описание	

В продукте kernel обнаружена уязвимость CVE-2018-20836.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140468
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140468>

BDU:2019-02826 (FSTEC)
<https://bdu.fstec.ru/vul/2019-02826>

RHSA-2021:0019 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:0019>

RHSA-2020:5656 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:5656>

CESA-2020:4060 (CESA-2020:4060)
<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2018-20836 (CVE)
 CVSSv2: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:I/C/A:C)
 CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
 CWE-362
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20836>

RHSA-2020:4062 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость	Риск: Средний
ALTX ID 337338	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-15217)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-15217.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140470
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140470>

BDU:2019-03091 (FSTEC)

<https://bdu.fstec.ru/vul/2019-03091>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2019-15217 (CVE)

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 4.5 (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15217>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость	Риск: Средний
ALTX ID 337339	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-15807)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-15807.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140471

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140471>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-02385 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02385>

CVE-2019-15807 (CVE)

CVSSv2: Базовая оценка 4.6 (AV:L/AC:M/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 4.6 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15807>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость	Риск: Средний
ALTX ID 337340	Red Hat/CentOS -- уязвимость в kernel (CVE-2019-15917)
Описание	

В продукте kernel обнаружена уязвимость CVE-2019-15917.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140472

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140472>

BDU:2020-01468 (FSTEC)

<https://bdu.fstec.ru/vul/2020-01468>

RHSA-2021:0019 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0019>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2019-15917 (CVE)

CVSSv2: Базовая оценка 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-15917>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALT X ID

337343

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-16994)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-16994.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140475

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140475>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-01063 (FSTEC)

<https://bdu.fstec.ru/vul/2020-01063>

CVE-2019-16994 (CVE)

CVSSv2: Базовая оценка 4.6 (AV:L/AC:M/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 4.6 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16994>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALT X ID

337344

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-18808)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-18808.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140476

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140476>

BDU:2019-04511 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04511>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2019-18808 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18808>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337345

Red Hat/CentOS -- уязвимость в kernel (CVE-2019-19046)

Описание

В продукте kernel обнаружена уязвимость CVE-2019-19046.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140477

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140477>

RHSA-2020:5656 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5656>

RHSA-2020:5206 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5206>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-01564 (FSTEC)<https://bdu.fstec.ru/vul/2020-01564>**CVE-2019-19046 (CVE)**

CVSSv2: Базовая оценка 6.8 (AV:N/AC:L/Au:S/C:N/I:N/A:C)

CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19046>**RHSA-2020:4062 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337346

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19055)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19055.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140478<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140478>**BDU:2019-04664 (FSTEC)**<https://bdu.fstec.ru/vul/2019-04664>**CESA-2020:4060 (CESA-2020:4060)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>**RHSA-2020:4060 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4060>**CVE-2019-19055 (CVE)**

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19055>**RHSA-2020:4062 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337347

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19058)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19058.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140479<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140479>**BDU:2019-04806 (FSTEC)**<https://bdu.fstec.ru/vul/2019-04806>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2019-19058 (CVE)

CVSSv2: Базовая оценка 4.6 (AV:L/AC:M/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 4.6 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19058>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337348

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19059)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19059.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140480

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140480>

BDU:2019-04811 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04811>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2019-19059 (CVE)

CVSSv2: Базовая оценка 4.6 (AV:L/AC:M/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 4.6 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19059>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337349

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19062)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19062.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140481

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140481>

BDU:2019-04802 (FSTEC)<https://bdu.fstec.ru/vul/2019-04802>**RHSA-2020:4609 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4609>**RHSA-2020:4431 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4431>**CESA-2020:4060 (CESA-2020:4060)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>**RHSA-2020:4060 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4060>**CVE-2019-19062 (CVE)**

CVSSv2: Базовая оценка 4.6 (AV:L/AC:M/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 4.6 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19062>**RHSA-2020:4062 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID
337350**Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19063)**

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19063.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140482<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140482>**BDU:2019-04801 (FSTEC)**<https://bdu.fstec.ru/vul/2019-04801>**RHSA-2020:4609 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4609>**RHSA-2020:4431 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4431>**CESA-2020:4060 (CESA-2020:4060)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>**RHSA-2020:4060 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4060>**CVE-2019-19063 (CVE)**

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 4.5 (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19063>**RHSA-2020:4062 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID
337351**Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19332)**

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19332.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140483

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140483>

BDU:2020-05893 (FSTEC)

<https://bdu.fstec.ru/vul/2020-05893>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2019-19332 (CVE)

CVSSv2: Базовая оценка 5.5 (AV:L/AC:L/Au:N/C:N/I:P/A:C)

CVSSv3: Базовая оценка 6.0 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19332>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337353

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19523)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19523.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140485

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140485>

RHSA-2021:1739 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1739>

RHSA-2021:1578 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1578>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-00292 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00292>

CVE-2019-19523 (CVE)

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)
CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CWE-416
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19523>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость	Риск: Средний
ALTX ID 337354	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19524)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19524.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140486
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140486>

RHSA-2020:4609 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)
<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-00290 (FSTEC)
<https://bdu.fstec.ru/vul/2020-00290>

CVE-2019-19524 (CVE)
CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)
CVSSv3: Базовая оценка 4.5 (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-416
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19524>

RHSA-2020:4062 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость	Риск: Средний
ALTX ID 337355	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19530)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19530.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140487
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140487>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-00286 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00286>

CVE-2019-19530 (CVE)

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 5.6 (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19530>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID
337357

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19767)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19767.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140489

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140489>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2019-19767 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19767>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID
337358

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-20054)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-20054.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140490

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140490>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-00357 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00357>

CVE-2019-20054 (CVE)

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 5.0 (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20054>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337359

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-20095)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-20095.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140491

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140491>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-00360 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00360>

CVE-2019-20095 (CVE)

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 5.1 (CVSS:3.1/AV:A/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20095>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337360

Red Hat/CentOS -- уязвимость в kernel (CVE-2019-20636)

Описание

В продукте kernel обнаружена уязвимость CVE-2019-20636.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140492

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140492>

BDU:2021-03056 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03056>

RHSA-2021:0019 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0019>

RHSA-2020:5656 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5656>

RHSA-2020:5430 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5430>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2019-20636 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 6.6 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20636>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALT X ID

337361

Red Hat/CentOS -- уязвимость в kernel (CVE-2019-9454)

Описание

В продукте kernel обнаружена уязвимость CVE-2019-9454.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140493

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140493>

RHSA-2020:5656 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5656>

RHSA-2020:5430 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5430>

RHSA-2020:5206 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5206>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2019-9454 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9454>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337362

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-9458)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-9458.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140494

<https://ovaldbrn.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140494>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2019-9458 (CVE)

CVSSv2: Базовая оценка 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-362

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9458>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337363

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10690)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-10690.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140495

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140495>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2020-10690 (CVE)

CVSSv2: Базовая оценка 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10690>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID
337365

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10742)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-10742.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140497

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140497>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-03364 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03364>

CVE-2020-10742 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:P/I:N/A:P)

CVSSv3: Базовая оценка 6.0 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10742>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID
337366

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10751)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-10751.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140498

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140498>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-03430 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03430>

CVE-2020-10751 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:P/I:P/A:N)

CVSSv3: Базовая оценка 6.0 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N)

CWE-349

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10751>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID
337368

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10942)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-10942.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140500

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140500>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-02707 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02707>

CVE-2020-10942 (CVE)

CVSSv2: Базовая оценка 5.4 (AV:L/AC:M/Au:N/C:N/I:P/A:C)

CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10942>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337392

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-11565)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-11565.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140524

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140524>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-02286 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02286>

CVE-2020-11565 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:N/I:P/A:P)

CVSSv3: Базовая оценка 6.0 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11565>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337393

Red Hat/CentOS -- уязвимость в kernel (CVE-2020-12770)

Описание

В продукте kernel обнаружена уязвимость CVE-2020-12770.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140525

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140525>

RHSA-2020:5656 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5656>

RHSA-2020:5430 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5430>

RHSA-2020:5206 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5206>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-02431 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02431>

CVE-2020-12770 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 6.6 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12770>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALT X ID

337394

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-12826)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-12826.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140526

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140526>

BDU:2021-00466 (FSTEC)

<https://bdu.fstec.ru/vul/2021-00466>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2020-12826 (CVE)

CVSSv2: Базовая оценка 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12826>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALT X ID

337404

Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2020-8647)

Описание

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2020-8647.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140536

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140536>

RHSA-2022:1209 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1209>

RHSA-2022:1213 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1213>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-00785 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00785>

CVE-2020-8647 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:P/I:N/A:P)

CVSSv3: Базовая оценка 6.0 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8647>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337405

Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2020-8649)

Описание

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2020-8649.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140537

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140537>

RHSA-2022:1209 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1209>

RHSA-2022:1213 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1213>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-00786 (FSTEC)<https://bdu.fstec.ru/vul/2020-00786>**CVE-2020-8649 (CVE)**

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:P/I:N/A:P)

CVSSv3: Базовая оценка 5.9 (CVSS:3.1/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8649>**RHSA-2020:4062 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337406

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-9383)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-9383.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140538<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140538>**CESA-2020:4060 (CESA-2020:4060)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>**RHSA-2020:4060 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4060>**BDU:2020-01075 (FSTEC)**<https://bdu.fstec.ru/vul/2020-01075>**CVE-2020-9383 (CVE)**

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:P/I:N/A:P)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9383>**RHSA-2020:4062 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Средний

ALTX ID

337757

Red Hat/CentOS -- уязвимость в cups (CVE-2017-18190)

Описание

В продукте cups обнаружена уязвимость CVE-2017-18190.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140824<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140824>**BDU:2018-01423 (FSTEC)**<https://bdu.fstec.ru/vul/2018-01423>

CESA-2020:3864 (CESA-2020:3864)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012674.html>

CVE-2017-18190 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 5.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:L)

CWE-290

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18190>

RHSA-2020:3864 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3864>

Уязвимость

Риск: Средний

ALTX ID

337759

Red Hat/CentOS -- уязвимость в httpd (CVE-2018-1283)

Описание

В продукте httpd обнаружена уязвимость CVE-2018-1283.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140826

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140826>

BDU:2019-04308 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04308>

CESA-2020:3958 (CESA-2020:3958)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012727.html>

CVE-2018-1283 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:N/AC:M/Au:S/C:N/I:P/A:N)

CVSSv3: Базовая оценка 4.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1283>

RHSA-2020:3958 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3958>

Уязвимость

Риск: Средний

ALTX ID

337760

Red Hat/CentOS -- уязвимость в httpd (CVE-2018-1303)

Описание

В продукте httpd обнаружена уязвимость CVE-2018-1303.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140827

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140827>

BDU:2019-04310 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04310>

CESA-2020:3958 (CESA-2020:3958)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012727.html>

CVE-2018-1303 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
 CVSSv3: Базовая оценка 5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
 CWE-125
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1303>

RHSA-2020:3958 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3958>

Уязвимость	Риск: Средний
ALTX ID 337777	Red Hat/CentOS -- уязвимость в срpio (CVE-2019-14866)
Описание	

В продукте срpio обнаружена уязвимость CVE-2019-14866.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140844
<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140844>

RHSA-2022:0073 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0073>

RHSA-2021:1582 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1582>

CESA-2020:3908 (CESA-2020:3908)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012671.html>

BDU:2020-01329 (FSTEC)

<https://bdu.fstec.ru/vul/2020-01329>

CVE-2019-14866 (CVE)

CVSSv2: Базовая оценка 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)
 CVSSv3: Базовая оценка 6.6 (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H)
 CWE-20
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14866>

RHSA-2020:3908 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3908>

Уязвимость	Риск: Средний
ALTX ID 337779	Red Hat/CentOS -- уязвимость в python3 (CVE-2019-16935)
Описание	

В продукте python3 обнаружена уязвимость CVE-2019-16935.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140846
<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140846>

RHSA-2020:4433 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4433>

CESA-2020:3888 (CESA-2020:3888)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012810.html>

CESA-2020:3911 (CESA-2020:3911)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012809.html>

BDU:2020-04508 (FSTEC)

<https://bdu.fstec.ru/vul/2020-04508>

CVE-2019-16935 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 6.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CWE-79

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16935>

RHSA-2020:3888 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3888>

RHSA-2020:3911 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3911>

Уязвимость	Риск: Средний
ALTX ID 337783	Red Hat/CentOS -- уязвимость в libssh2 (CVE-2019-17498)
Описание	

В продукте libssh2 обнаружена уязвимость CVE-2019-17498.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140850

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140850>

BDU:2022-05961 (FSTEC)

<https://bdu.fstec.ru/vul/2022-05961>

CESA-2020:3915 (CESA-2020:3915)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012761.html>

CVE-2019-17498 (CVE)

CVSSv2: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:P/I:N/A:P)

CVSSv3: Базовая оценка 6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17498>

RHSA-2020:3915 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3915>

Уязвимость	Риск: Средний
ALTX ID 337787	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2019-19956)
Описание	

В продукте libxml2 обнаружена уязвимость CVE-2019-19956.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140854

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140854>

VULN-20220727.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.2.pdf>

RHSA-2020:4479 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4479>

CESA-2020:3996 (CESA-2020:3996)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012767.html>

BDU:2020-04513 (FSTEC)

<https://bdu.fstec.ru/vul/2020-04513>

CVE-2019-19956 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19956>

RHSA-2020:3996 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3996>

Уязвимость

Риск: Средний

ALTX ID

337789

Red Hat/CentOS -- уязвимость в libxml2 (CVE-2019-20388)

Описание

В продукте libxml2 обнаружена уязвимость CVE-2019-20388.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140856

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140856>

VULN-20220727.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.2.pdf>

RHSA-2020:4479 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4479>

CESA-2020:3996 (CESA-2020:3996)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012767.html>

BDU:2020-04514 (FSTEC)

<https://bdu.fstec.ru/vul/2020-04514>

CVE-2019-20388 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20388>

RHSA-2020:3996 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3996>

Уязвимость

Риск: Средний

ALTX ID

337911

Red Hat/CentOS -- уязвимость в openldap (CVE-2020-12243)

Описание

В продукте openldap обнаружена уязвимость CVE-2020-12243.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140978

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140978>

CESA-2020:4041 (CESA-2020:4041)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012791.html>

CVE-2020-12243 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-674

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12243>

RHSA-2020:4041 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4041>

Уязвимость

Риск: Средний

ALT X ID

337914

Red Hat/CentOS -- уязвимость в nspr, nss, nss-softokn (CVE-2020-12403)

Описание

В продуктах nspr, nss, nss-softokn обнаружена уязвимость CVE-2020-12403.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140981

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140981>

CESA-2020:4076-CentOS 7 (CESA-2020:4076)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-November/012876.html>

RHSA-2021:1026 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1026>

RHSA-2021:0876 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0876>

RHSA-2021:0758 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0758>

RHSA-2021:0538 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0538>

CVE-2020-12403 (CVE)

CVSSv2: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P)

CVSSv3: Базовая оценка 9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12403>

RHSA-2020:4076 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4076>

Уязвимость

Риск: Средний

ALT X ID

337931

Red Hat/CentOS -- уязвимость в httpd:2.4 (CVE-2020-1927)

Описание

В продукте httpd:2.4 обнаружена уязвимость CVE-2020-1927.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140998

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140998>

RHSA-2020:4751 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4751>

CESA-2020:3958 (CESA-2020:3958)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012727.html>

BDU:2020-03569 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03569>

CVE-2020-1927 (CVE)

CVSSv2: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSSv3: Базовая оценка 6.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

CWE-601

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1927>

RHSA-2020:3958 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3958>

Уязвимость

Риск: Средний

ALTX ID

337979

Red Hat/CentOS -- уязвимость в libxml2 (CVE-2020-7595)

Описание

В продукте libxml2 обнаружена уязвимость CVE-2020-7595.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:141046

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:141046>

VULN-20220727.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.2.pdf>

RHSA-2020:4479 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4479>

CESA-2020:3996 (CESA-2020:3996)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012767.html>

BDU:2020-03623 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03623>

CVE-2020-7595 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-835

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7595>

RHSA-2020:3996 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3996>

Уязвимость

Риск: Средний

ALTX ID

337981

Red Hat/CentOS -- уязвимость в Bind (CVE-2020-8622)

Описание

В продукте Bind обнаружена уязвимость CVE-2020-8622.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:141048

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:141048>

CESA-2020:4183 (CESA-2020:4183)

<http://lists.centos.org/pipermail/centos-announce/2020-November/035814.html>

CESA-2020:5011 (CESA-2020:5011)

<http://lists.centos.org/pipermail/centos-announce/2020-November/035850.html>

BDU:2021-01725 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01725>

RHSA-2020:5203 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5203>

RHSA-2020:4500 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4500>

RHSA-2020:5011 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5011>

RHSA-2020:4992 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4992>

CVE-2020-8622 (CVE)

CVSSv2: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)

CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-617

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8622>

RHSA-2020:4183 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4183>

Уязвимость

Риск: Средний

ALTX ID

339336

Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2020-14331)

Описание

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2020-14331.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:141668

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:141668>

BDU:2023-00700 (FSTEC)

<https://bdu.fstec.ru/vul/2023-00700>

CESA-2020:5023 (CESA-2020:5023)

<http://lists.centos.org/pipermail/centos-announce/2020-November/035868.html>

RHSA-2020:5023 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5023>

RHSA-2020:5026 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5026>

CVE-2020-14331 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14331>

RHSA-2020:4286 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4286>

RHSA-2020:4289 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4289>

Уязвимость	Риск: Средний
ALTX ID 339337	Red Hat/CentOS -- уязвимость в kernel, kernel-rt, kpatch-patch (CVE-2020-14385)
Описание	

В продуктах kernel, kernel-rt, kpatch-patch обнаружена уязвимость CVE-2020-14385.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:141669

<https://ovaldbr.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:141669>

RHSA-2020:5199 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5199>

CESA-2020:5437 (CESA-2020:5437)

<http://lists.centos.org/pipermail/centos-announce/2020-December/048241.html>

RHSA-2020:5441 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5441>

RHSA-2020:5437 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5437>

RHSA-2020:5050 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5050>

RHSA-2020:4331 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4331>

RHSA-2020:4332 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4332>

BDU:2020-04339 (FSTEC)

<https://bdu.fstec.ru/vul/2020-04339>

CVE-2020-14385 (CVE)

CVSSv2: Базовая оценка 4.6 (AV:L/AC:M/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 6.1 (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-131

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14385>

RHSA-2020:4286 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4286>

RHSA-2020:4287 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4287>

RHSA-2020:4289 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4289>

Уязвимость	Риск: Средний
ALT X ID 341338	Red Hat/CentOS -- уязвимость в python38:3.8, python3, python27:2.7, Python (CVE-2019-20907)
Описание	В продукте python38:3.8, python3, python27:2.7, Python обнаружена уязвимость CVE-2019-20907.
Исправление	Необходимо установить актуальное обновление от производителя.
Ссылки	<p>oval:ru.altx-soft.nix:def:143026 https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:143026</p> <p>CESA-2020:5010 (CESA-2020:5010) http://lists.centos.org/pipermail/centos-announce/2020-November/035824.html</p> <p>CESA-2020:5009 (CESA-2020:5009) http://lists.centos.org/pipermail/centos-announce/2020-November/035822.html</p> <p>RHSA-2021:0881 (VENDOR) https://access.redhat.com/errata/RHSA-2021:0881</p> <p>RHSA-2021:0761 (VENDOR) https://access.redhat.com/errata/RHSA-2021:0761</p> <p>RHSA-2021:0528 (VENDOR) https://access.redhat.com/errata/RHSA-2021:0528</p> <p>BDU:2021-00726 (FSTEC) https://bdu.fstec.ru/vul/2021-00726</p> <p>CVE-2019-20907 (CVE) CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P) CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) CWE-835 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20907</p> <p>RHSA-2020:4641 (VENDOR) https://access.redhat.com/errata/RHSA-2020:4641</p> <p>RHSA-2020:4433 (VENDOR) https://access.redhat.com/errata/RHSA-2020:4433</p> <p>RHSA-2020:4654 (VENDOR) https://access.redhat.com/errata/RHSA-2020:4654</p> <p>RHSA-2020:5010 (VENDOR) https://access.redhat.com/errata/RHSA-2020:5010</p> <p>RHSA-2020:5009 (VENDOR) https://access.redhat.com/errata/RHSA-2020:5009</p>

Уязвимость	Риск: Средний
ALT X ID 341348	Red Hat/CentOS -- уязвимость в glibc (CVE-2020-10029)
Описание	В продукте glibc обнаружена уязвимость CVE-2020-10029.
Исправление	Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:143036

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:143036>

RHSA-2021:3315 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3315>

RHSA-2021:2998 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2998>

CESA-2021:0348 (CESA-2021:0348)

<http://lists.centos.org/pipermail/centos-announce/2021-February/048257.html>

RHSA-2021:0348 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0348>

BDU:2020-04684 (FSTEC)

<https://bdu.fstec.ru/vul/2020-04684>

CVE-2020-10029 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 5.6 (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10029>

RHSA-2020:4444 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4444>

Уязвимость

Риск: Средний

ALTX ID

341363

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-11668)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-11668.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:143051

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:143051>

RHSA-2021:2726 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2726>

RHSA-2021:2725 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2725>

CESA-2021:2725 (CESA-2021:2725)

<http://lists.centos.org/pipermail/centos-announce/2021-July/048344.html>

BDU:2020-02136 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02136>

CVE-2020-11668 (CVE)

CVSSv2: Базовая оценка 5.5 (AV:L/AC:L/Au:N/C:N/I:P/A:C)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11668>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

Уязвимость

Риск: Средний

ALTX ID

341419

Red Hat/CentOS -- уязвимость в curl (CVE-2020-8177)

Описание

В продукте curl обнаружена уязвимость CVE-2020-8177.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:143107

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:143107>

CESA-2020:5002 (CESA-2020:5002)

<http://lists.centos.org/pipermail/centos-announce/2020-November/035840.html>

RHSA-2020:5417 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5417>

BDU:2020-03241 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03241>

CVE-2020-8177 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 5.4 (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:H/A:L)

CWE-74

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8177>

RHSA-2020:4599 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4599>

RHSA-2020:5002 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5002>

Уязвимость

Риск: Средний

ALTX ID

341421

Red Hat/CentOS -- уязвимость в Bind (CVE-2020-8623)

Описание

В продукте Bind обнаружена уязвимость CVE-2020-8623.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:143109

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:143109>

CESA-2020:5011 (CESA-2020:5011)

<http://lists.centos.org/pipermail/centos-announce/2020-November/035850.html>

BDU:2021-01693 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01693>

RHSA-2020:5203 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5203>

CVE-2020-8623 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-617

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8623>

RHSA-2020:4500 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:4500>**RHSA-2020:5011 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5011>**RHSA-2020:4992 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4992>

Уязвимость

Риск: Средний

ALTX ID
341423**Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2020-8648)****Описание**

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2020-8648.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:143111

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:143111>**RHSA-2021:3522 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3522>**RHSA-2021:3320 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3320>**CESA-2021:2314 (CESA-2021:2314)**<http://lists.centos.org/pipermail/centos-announce/2021-June/048337.html>**RHSA-2021:2316 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2316>**RHSA-2021:2314 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2314>**BDU:2020-00787 (FSTEC)**<https://bdu.fstec.ru/vul/2020-00787>**CVE-2020-8648 (CVE)**

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:P/I:N/A:P)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8648>**RHSA-2020:4609 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4609>**RHSA-2020:4431 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4431>

Уязвимость

Риск: Средний

ALTX ID
341424**Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-8695)****Описание**

В продукте microcode_ctl обнаружена уязвимость CVE-2020-8695.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:143112

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:143112>

RHSA-2020:5186 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5186>

RHSA-2021:3364 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3364>

RHSA-2021:3322 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3322>

RHSA-2021:3317 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3317>

RHSA-2021:3323 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3323>

RHSA-2021:3176 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3176>

RHSA-2021:3255 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3255>

RHSA-2021:3028 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3028>

CESA-2021:3028 (CESA-2021:3028)

<http://lists.centos.org/pipermail/centos-announce/2021-August/048347.html>

RHSA-2021:3029 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3029>

RHSA-2021:3027 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3027>

CESA-2020:5083 (CESA-2020:5083)

<http://lists.centos.org/pipermail/centos-announce/2020-November/035872.html>

RHSA-2020:5369 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5369>

BDU:2020-05482 (FSTEC)

<https://bdu.fstec.ru/vul/2020-05482>

RHSA-2020:5181 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5181>

RHSA-2020:5182 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5182>

RHSA-2020:5183 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5183>

RHSA-2020:5185 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5185>

RHSA-2020:5188 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5188>

RHSA-2020:5190 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5190>

CVE-2020-8695 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 5.0 (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

CWE-203

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8695>

RHSA-2020:5083 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5083>

RHSA-2020:5085 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5085>

Уязвимость

Риск: Средний

ALTX ID

341426

Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-8698)

Описание

В продукте microcode_ctl обнаружена уязвимость CVE-2020-8698.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:143114

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:143114>

RHSA-2020:5186 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5186>

RHSA-2021:3364 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3364>

RHSA-2021:3322 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3322>

RHSA-2021:3317 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3317>

RHSA-2021:3323 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3323>

RHSA-2021:3176 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3176>

RHSA-2021:3255 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3255>

RHSA-2021:3028 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3028>

CESA-2021:3028 (CESA-2021:3028)

<http://lists.centos.org/pipermail/centos-announce/2021-August/048347.html>

RHSA-2021:3029 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3029>

RHSA-2021:3027 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3027>

CESA-2020:5083 (CESA-2020:5083)

<http://lists.centos.org/pipermail/centos-announce/2020-November/035872.html>

RHSA-2020:5369 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5369>

BDU:2020-05479 (FSTEC)

<https://bdu.fstec.ru/vul/2020-05479>

RHSA-2020:5181 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5181>

RHSA-2020:5182 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5182>

RHSA-2020:5183 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5183>

RHSA-2020:5184 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5184>

RHSA-2020:5185 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5185>

RHSA-2020:5188 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5188>

RHSA-2020:5189 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:5189>**RHSA-2020:5190 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5190>**CVE-2020-8698 (CVE)**

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CWE-668

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8698>**RHSA-2020:5083 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5083>**RHSA-2020:5084 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5084>**RHSA-2020:5085 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5085>

Уязвимость

Риск: Средний

ALTX ID
343984**Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-18282)**

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-18282.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:145156<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:145156>**CESA-2020:5437 (CESA-2020:5437)**<http://lists.centos.org/pipermail/centos-announce/2020-December/048241.html>**BDU:2020-00362 (FSTEC)**<https://bdu.fstec.ru/vul/2020-00362>**CVE-2019-18282 (CVE)**

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CWE-330

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-18282>**RHSA-2020:5441 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5441>**RHSA-2020:5437 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5437>

Уязвимость

Риск: Средний

ALTX ID
343987**Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10769)**

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-10769.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:145159

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:145159>

CESA-2020:5437 (CESA-2020:5437)

<http://lists.centos.org/pipermail/centos-announce/2020-December/048241.html>

BDU:2020-03918 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03918>

CVE-2020-10769 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10769>

RHSA-2020:5441 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5441>

RHSA-2020:5437 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5437>

Уязвимость

Риск: Средний

ALTX ID

343991

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-14314)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-14314.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:145163

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:145163>

CESA-2020:5437 (CESA-2020:5437)

<http://lists.centos.org/pipermail/centos-announce/2020-December/048241.html>

RHSA-2021:1739 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1739>

RHSA-2021:1578 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1578>

CVE-2020-14314 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14314>

RHSA-2020:5441 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5441>

RHSA-2020:5437 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5437>

Уязвимость

Риск: Средний

ALTX ID

344005

Red Hat/CentOS -- уязвимость в OpenSSL (CVE-2020-1971)

Описание

В продукте OpenSSL обнаружена уязвимость CVE-2020-1971.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:145177

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:145177>

CESA-2020:5566 (CESA-2020:5566)

<http://lists.centos.org/pipermail/centos-announce/2020-December/048211.html>

RHSA-2020:5422 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5422>

BDU:2021-00872 (FSTEC)

<https://bdu.fstec.ru/vul/2021-00872>

RHSA-2021:0056 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0056>

RHSA-2020:5623 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5623>

RHSA-2020:5637 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5637>

RHSA-2020:5639 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5639>

RHSA-2020:5640 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5640>

RHSA-2020:5641 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5641>

RHSA-2020:5642 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5642>

CVE-2020-1971 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1971>

RHSA-2020:5476 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5476>

RHSA-2020:5566 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5566>

Уязвимость

Риск: Средний

ALTX ID
344006

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-24394)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-24394.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:145178

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:145178>

BDU:2021-03188 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03188>

CESA-2020:5437 (CESA-2020:5437)

<http://lists.centos.org/pipermail/centos-announce/2020-December/048241.html>

RHSA-2021:1739 (VENDOR)<https://access.redhat.com/errata/RHSA-2021:1739>**RHSA-2021:1578 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:1578>**RHSA-2021:0878 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0878>**RHSA-2021:0760 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0760>**RHSA-2021:0526 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0526>**CVE-2020-24394 (CVE)**

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:P/I:P/A:N)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N)

CWE-732

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24394>**RHSA-2020:5441 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5441>**RHSA-2020:5437 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5437>

Уязвимость

Риск: Средний

ALT X ID

344009

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-25212)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-25212.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:145181<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:145181>**CESA-2020:5437 (CESA-2020:5437)**<http://lists.centos.org/pipermail/centos-announce/2020-December/048241.html>**RHSA-2021:1739 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:1739>**RHSA-2021:1578 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:1578>**RHSA-2021:0878 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0878>**RHSA-2021:0760 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0760>**RHSA-2021:0526 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0526>**BDU:2020-05723 (FSTEC)**<https://bdu.fstec.ru/vul/2020-05723>**CVE-2020-25212 (CVE)**

CVSSv2: Базовая оценка 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25212>**RHSA-2020:5441 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5441>

RHSA-2020:5437 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:5437>

Уязвимость	Риск: Средний
ALT X ID 344010	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-25643)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-25643.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:145182**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:145182>**CESA-2020:5437 (CESA-2020:5437)**<http://lists.centos.org/pipermail/centos-announce/2020-December/048241.html>**RHSA-2021:1739 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:1739>**RHSA-2021:1578 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:1578>**BDU:2021-00106 (FSTEC)**<https://bdu.fstec.ru/vul/2021-00106>**CVE-2020-25643 (CVE)**

CVSSv2: Базовая оценка 7.5 (AV:N/AC:M/Au:S/C:P/I:P/A:C)

CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)

CWE-20

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25643>**RHSA-2020:5441 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5441>**RHSA-2020:5437 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:5437>

Уязвимость	Риск: Средний
ALT X ID 344758	Red Hat/CentOS -- уязвимость в kernel (CVE-2020-25211)

Описание

В продукте kernel обнаружена уязвимость CVE-2020-25211.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:145809**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:145809>**RHSA-2021:0774 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0774>**RHSA-2021:2355 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2355>

RHSA-2021:2164 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2164>

CESA-2021:0856 (CESA-2021:0856)

<http://lists.centos.org/pipermail/centos-announce/2021-March/048295.html>

RHSA-2021:1531 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1531>

RHSA-2021:0857 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0857>

RHSA-2021:0856 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0856>

RHSA-2021:0763 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0763>

RHSA-2021:0765 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0765>

RHSA-2021:0184 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0184>

RHSA-2021:0189 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0189>

CVE-2020-25211 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:N/I:P/A:P)

CVSSv3: Базовая оценка 6.6 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)

CWE-120

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25211>

RHSA-2021:0003 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0003>

RHSA-2021:0004 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0004>

Уязвимость	Риск: Средний
ALTX ID 347610	Red Hat/CentOS -- уязвимость в glibc (CVE-2019-25013)

Описание

В продукте glibc обнаружена уязвимость CVE-2019-25013.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:147127

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:147127>

BDU:2021-03123 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03123>

CESA-2021:0348 (CESA-2021:0348)

<http://lists.centos.org/pipermail/centos-announce/2021-February/048257.html>

RHSA-2021:1585 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1585>

CVE-2019-25013 (CVE)

CVSSv2: Базовая оценка 7.0 (AV:N/AC:M/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-25013>

RHSA-2021:0348 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0348>

Уязвимость

Риск: Средний

ALTX ID
347613

Red Hat/CentOS -- уязвимость в perl (CVE-2020-12723)

Описание

В продукте perl обнаружена уязвимость CVE-2020-12723.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:147130

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:147130>

RHSA-2021:2184 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2184>

CESA-2021:0343 (CESA-2021:0343)

<http://lists.centos.org/pipermail/centos-announce/2021-February/048259.html>

RHSA-2021:1266 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1266>

RHSA-2021:1032 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1032>

RHSA-2021:0883 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0883>

RHSA-2021:0557 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0557>

BDU:2020-04041 (FSTEC)

<https://bdu.fstec.ru/vul/2020-04041>

CVE-2020-12723 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-120

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12723>

RHSA-2021:0343 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0343>

Уязвимость

Риск: Средний

ALTX ID
347617

Red Hat/CentOS -- уязвимость в glibc (CVE-2020-29573)

Описание

В продукте glibc обнаружена уязвимость CVE-2020-29573.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:147134

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:147134>

RHSA-2021:3315 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3315>

RHSA-2021:2998 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2998>

RHSA-2021:2813 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2813>

CESA-2021:0348 (CESA-2021:0348)

<http://lists.centos.org/pipermail/centos-announce/2021-February/048257.html>

CVE-2020-29573 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29573>

RHSA-2021:0348 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0348>

Уязвимость	Риск: Средний
ALTX ID 348237	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-14351)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-14351.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:147488

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:147488>

RHSA-2021:0774 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0774>

CESA-2021:0856 (CESA-2021:0856)

<http://lists.centos.org/pipermail/centos-announce/2021-March/048295.html>

RHSA-2021:0558 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0558>

RHSA-2021:1267 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1267>

RHSA-2021:1028 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1028>

RHSA-2021:0878 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0878>

RHSA-2021:0857 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0857>

RHSA-2021:0856 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0856>

RHSA-2021:0848 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0848>

RHSA-2021:0765 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0765>

RHSA-2021:0686 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0686>

BDU:2020-05832 (FSTEC)

<https://bdu.fstec.ru/vul/2020-05832>

CVE-2020-14351 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CWE-416
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14351>

RHSA-2021:0537 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0537>

Уязвимость	Риск: Средний
ALTX ID 348239	Red Hat/CentOS -- уязвимость в kernel (CVE-2020-25705)
Описание	

В продукте kernel обнаружена уязвимость CVE-2020-25705.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

- oval:ru.altx-soft.nix:def:147490**
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:147490>
- RHSA-2021:0774 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:0774>
- RHSA-2021:2355 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2355>
- RHSA-2021:2164 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2164>
- CESA-2021:0856 (CESA-2021:0856)**
<http://lists.centos.org/pipermail/centos-announce/2021-March/048295.html>
- RHSA-2021:0558 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:0558>
- RHSA-2021:1531 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:1531>
- RHSA-2021:0857 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:0857>
- RHSA-2021:0856 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:0856>
- RHSA-2021:0765 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:0765>
- RHSA-2021:0686 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:0686>
- BDU:2020-05539 (FSTEC)**
<https://bdu.fstec.ru/vul/2020-05539>
- CVE-2020-25705 (CVE)**
CVSSv2: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)
CVSSv3: Базовая оценка 7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)
CWE-330
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25705>
- RHSA-2021:0537 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:0537>

Уязвимость	Риск: Средний
------------	---------------

ALTX ID

349343

Red Hat/CentOS -- уязвимость в wpa_supplicant (CVE-2021-27803)

Описание

В продукте wpa_supplicant обнаружена уязвимость CVE-2021-27803.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:148088

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148088>

CESA-2021:0808 (CESA-2021:0808)

<http://lists.centos.org/pipermail/centos-announce/2021-March/048292.html>

BDU:2021-01584 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01584>

RHSA-2021:0818 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0818>

RHSA-2021:0816 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0816>

CVE-2021-27803 (CVE)

CVSSv2: Базовая оценка 5.4 (AV:A/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27803>

RHSA-2021:0808 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0808>

RHSA-2021:0809 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0809>

Уязвимость

Риск: Средний

ALTX ID

350025

Red Hat/CentOS -- уязвимость в kernel (CVE-2019-19532)

Описание

В продукте kernel обнаружена уязвимость CVE-2019-19532.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:148598

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148598>

RHSA-2021:2355 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2355>

RHSA-2021:2164 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2164>

CESA-2021:0856 (CESA-2021:0856)

<http://lists.centos.org/pipermail/centos-announce/2021-March/048295.html>

RHSA-2021:1531 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1531>

BDU:2020-00369 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00369>

CVE-2019-19532 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)
 CVSSv3: Базовая оценка 6.8 (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
 CWE-787
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19532>

RHSA-2021:0857 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0857>

RHSA-2021:0856 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0856>

Уязвимость	Риск: Средний
ALTX ID	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-0427)
350026	
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-0427.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

- oval:ru.altx-soft.nix:def:148599
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148599>
- RHSA-2021:4140 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4140>
- RHSA-2021:4356 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4356>
- CESA-2021:0856 (CESA-2021:0856)**
<http://lists.centos.org/pipermail/centos-announce/2021-March/048295.html>
- BDU:2020-05785 (FSTEC)**
<https://bdu.fstec.ru/vul/2020-05785>
- CVE-2020-0427 (CVE)**
 CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)
 CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)
 CWE-125
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0427>
- RHSA-2021:0857 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:0857>
- RHSA-2021:0856 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:0856>

Уязвимость	Риск: Средний
ALTX ID	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-7053)
350031	
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-7053.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:148604

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148604>

CESA-2021:0856 (CESA-2021:0856)

<http://lists.centos.org/pipermail/centos-announce/2021-March/048295.html>

BDU:2020-00361 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00361>

CVE-2020-7053 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7053>

RHSA-2021:0857 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0857>

RHSA-2021:0856 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0856>

Уязвимость

Риск: Средний

ALTX ID
350033

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2021-20265)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2021-20265.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:148606

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148606>

CESA-2021:0856 (CESA-2021:0856)

<http://lists.centos.org/pipermail/centos-announce/2021-March/048295.html>

RHSA-2021:1288 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1288>

BDU:2021-01684 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01684>

CVE-2021-20265 (CVE)

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20265>

RHSA-2021:0857 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0857>

RHSA-2021:0856 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0856>

Уязвимость

Риск: Средний

ALTX ID
350443

Red Hat/CentOS -- уязвимость в kernel, kernel-rt, kpatch-patch-3_10_0-1062_46_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_70_1, kpatch-patch-4_18_0-147_20_1, kpatch-patch-4_18_0-193_13_2 (CVE-2020-0466)

Описание

В продукте kernel, kernel-rt, kpatch-patch-3_10_0-1062_46_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_70_1, kpatch-patch-4_18_0-147_20_1, kpatch-patch-4_18_0-193_13_2 обнаружена уязвимость CVE-2020-0466.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:148870

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148870>

RHSA-2021:2190 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2190>

RHSA-2022:0712 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0712>

RHSA-2022:1417 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1417>

RHSA-2022:1104 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1104>

CESA-2022:0620 (CESA-2022:0620)

<http://lists.centos.org/pipermail/centos-announce/2022-February/073573.html>

RHSA-2022:0718 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0718>

RHSA-2022:0592 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0592>

RHSA-2022:0620 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0620>

RHSA-2022:0622 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0622>

RHSA-2022:0529 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0529>

RHSA-2022:0531 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0531>

RHSA-2022:0533 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0533>

RHSA-2021:2167 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2167>

RHSA-2021:2185 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2185>

RHSA-2021:2106 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2106>

RHSA-2021:2099 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2099>

RHSA-2021:1093 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1093>

CVE-2020-0466 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0466>

RHSA-2021:1081 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1081>

Уязвимость

Риск: Средний

ALT X ID
350456

Red Hat/CentOS -- уязвимость в kernel (CVE-2021-27363)

Описание

В продукте kernel обнаружена уязвимость CVE-2021-27363.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:148883

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148883>

RHSA-2021:1279 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1279>

RHSA-2021:1531 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1531>

RHSA-2021:1272 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1272>

RHSA-2021:1373 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1373>

RHSA-2021:1376 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1376>

RHSA-2021:1267 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1267>

RHSA-2021:1289 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1289>

CESA-2021:1071 (CESA-2021:1071)

<http://lists.centos.org/pipermail/centos-announce/2021-April/048298.html>

RHSA-2021:1171 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1171>

RHSA-2021:1093 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1093>

BDU:2021-01649 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01649>

BDU:2021-01266 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01266>

CVE-2021-27363 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:P/I:N/A:P)

CVSSv3: Базовая оценка 4.4 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27363>

RHSA-2021:1081 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1081>

RHSA-2021:1071 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1071>

RHSA-2021:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1070>

Уязвимость

Риск: Средний

ALT X ID
350457

Red Hat/CentOS -- уязвимость в kernel, kpatch-patch-4_18_0-193, kpatch-patch-4_18_0-193_1_2, kpatch-patch-4_18_0-193_6_3, kpatch-patch-4_18_0-193_13_2, kpatch-patch-4_18_0-193_14_3, kpatch-patch-4_18_0-193_19_1, kpatch-patch-4_18_0-193_28_1, kpatch-patch-4_18_0-193_29_1, kpatch-patch-4_18_0-193_37_1, kpatch-patch-4_18_0-193_40_1, kpatch-patch-4_18_0-193_41_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-3_10_0-957_54_1, kpatch-patch-3_10_0-957_56_1, kpatch-patch-3_10_0-957_58_2, kpatch-patch-3_10_0-957_61_1, kpatch-patch-3_10_0-957_61_2, kpatch-patch-3_10_0-957_62_1, kpatch-patch-3_10_0-957_65_1, kpatch-patch-3_10_0-957_66_1, kpatch-patch-3_10_0-957_70_1, kpatch-patch-3_10_0-1062_26_1 (CVE-2021-27364)

Описание

В продукте kernel, kpatch-patch-4_18_0-193, kpatch-patch-4_18_0-193_1_2, kpatch-patch-4_18_0-193_6_3, kpatch-patch-4_18_0-193_13_2, kpatch-patch-4_18_0-193_14_3, kpatch-patch-4_18_0-193_19_1, kpatch-patch-4_18_0-193_28_1, kpatch-patch-4_18_0-193_29_1, kpatch-patch-4_18_0-193_37_1, kpatch-patch-4_18_0-193_40_1, kpatch-patch-4_18_0-193_41_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-3_10_0-957_54_1, kpatch-patch-3_10_0-957_56_1, kpatch-patch-3_10_0-957_58_2, kpatch-patch-3_10_0-957_61_1, kpatch-patch-3_10_0-957_61_2, kpatch-patch-3_10_0-957_62_1, kpatch-patch-3_10_0-957_65_1, kpatch-patch-3_10_0-957_66_1, kpatch-patch-3_10_0-957_70_1, kpatch-patch-3_10_0-1062_26_1 обнаружена уязвимость CVE-2021-27364.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:148884

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148884>

RHSA-2021:1279 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1279>

RHSA-2021:1531 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1531>

RHSA-2021:1532 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1532>

RHSA-2021:1272 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1272>

RHSA-2021:1373 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1373>

RHSA-2021:1376 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1376>

RHSA-2021:1377 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1377>

RHSA-2021:1267 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1267>

RHSA-2021:1288 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1288>

RHSA-2021:1289 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1289>

RHSA-2021:1295 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1295>

CESA-2021:1071 (CESA-2021:1071)

<http://lists.centos.org/pipermail/centos-announce/2021-April/048298.html>

RHSA-2021:1173 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1173>

RHSA-2021:1171 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1171>

RHSA-2021:1093 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1093>

BDU:2021-01650 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01650>

BDU:2021-01213 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01213>

CVE-2021-27364 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:P/I:N/A:P)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27364>

RHSA-2021:1069 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1069>

RHSA-2021:1081 (VENDOR)<https://access.redhat.com/errata/RHSA-2021:1081>**RHSA-2021:1071 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:1071>**RHSA-2021:1070 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:1070>

Уязвимость

Риск: Средний

ALTX ID
350459**Red Hat/CentOS -- уязвимость в kpatch-patch-3_10_0-1062_36_1, kernel, kpatch-patch-3_10_0-1160, kernel-rt, kpatch-patch-3_10_0-957_58_2, kpatch-patch-4_18_0-147_20_1, kpatch-patch-4_18_0-193, kpatch-patch-4_18_0-193_1_2, kpatch-patch-4_18_0-193_13_2, kpatch-patch-4_18_0-193_14_3, kpatch-patch-4_18_0-193_19_1, kpatch-patch-4_18_0-193_28_1, kpatch-patch-4_18_0-193_29_1, kpatch-patch-4_18_0-193_37_1, kpatch-patch-4_18_0-193_40_1, kpatch-patch-4_18_0-193_41_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-4_18_0-193_6_3 (CVE-2021-3347)****Описание**

В продукте kpatch-patch-3_10_0-1062_36_1, kernel, kpatch-patch-3_10_0-1160, kernel-rt, kpatch-patch-3_10_0-957_58_2, kpatch-patch-4_18_0-147_20_1, kpatch-patch-4_18_0-193, kpatch-patch-4_18_0-193_1_2, kpatch-patch-4_18_0-193_13_2, kpatch-patch-4_18_0-193_14_3, kpatch-patch-4_18_0-193_19_1, kpatch-patch-4_18_0-193_28_1, kpatch-patch-4_18_0-193_29_1, kpatch-patch-4_18_0-193_37_1, kpatch-patch-4_18_0-193_40_1, kpatch-patch-4_18_0-193_41_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-4_18_0-193_6_3 обнаружена уязвимость CVE-2021-3347.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:148886**<https://ovaldbrn.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148886>**RHSA-2021:1279 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:1279>**RHSA-2021:3523 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3523>**RHSA-2021:3522 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3522>**RHSA-2021:3399 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3399>**RHSA-2021:2285 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2285>**RHSA-2021:2730 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2730>**RHSA-2021:2733 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2733>**RHSA-2021:2735 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2735>**RHSA-2021:2732 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2732>**RHSA-2021:2731 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2731>**CESA-2021:2314 (CESA-2021:2314)**<http://lists.centos.org/pipermail/centos-announce/2021-June/048337.html>**RHSA-2021:2316 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2316>**RHSA-2021:2314 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2314>

RHSA-2021:2106 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2106>

RHSA-2021:2099 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2099>

BDU:2021-02593 (FSTEC)

<https://bdu.fstec.ru/vul/2021-02593>

RHSA-2021:1272 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1272>

RHSA-2021:1295 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1295>

RHSA-2021:1093 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1093>

CVE-2021-3347 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3347>

RHSA-2021:1081 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1081>

Уязвимость	Риск: Средний
ALT X ID	Red Hat/CentOS -- уязвимость в Bind (CVE-2021-25215)
355759	
Описание	

В продукте Bind обнаружена уязвимость CVE-2021-25215.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:153186

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:153186>

VULN-20220906.7 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220906.7.pdf>

VULN-20220110.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220110.2.pdf>

BDU:2021-02778 (FSTEC)

<https://bdu.fstec.ru/vul/2021-02778>

RHSA-2021:1468 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1468>

RHSA-2021:1469 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1469>

CESA-2021:1469 (CESA-2021:1469)

<http://lists.centos.org/pipermail/centos-announce/2021-April/048313.html>

RHSA-2021:1989 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1989>

RHSA-2021:2024 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2024>

RHSA-2021:2028 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2028>

CVE-2021-25215 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
 CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
 CWE-617
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25215>

RHSA-2021:1479 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1479>

RHSA-2021:1478 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1478>

RHSA-2021:1477 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1477>

RHSA-2021:1476 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1476>

RHSA-2021:1475 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1475>

Уязвимость	Риск: Средний
ALTX ID 357270	Red Hat/CentOS -- уязвимость в kernel (CVE-2020-12362)
Описание	

В продукте kernel обнаружена уязвимость CVE-2020-12362.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

- oval:ru.altx-soft.nix:def:153632**
<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:153632>
- RHSA-2021:2190 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2190>
- RHSA-2021:2735 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2735>
- CESA-2021:2314 (CESA-2021:2314)**
<http://lists.centos.org/pipermail/centos-announce/2021-June/048337.html>
- RHSA-2021:2523 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2523>
- RHSA-2021:2293 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2293>
- RHSA-2021:2316 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2316>
- RHSA-2021:2314 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2314>
- RHSA-2021:2355 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2355>
- RHSA-2021:2185 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2185>
- RHSA-2021:2164 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2164>
- BDU:2021-00871 (FSTEC)**
<https://bdu.fstec.ru/vul/2021-00871>
- RHSA-2021:2106 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:2106>

CVE-2020-12362 (CVE)

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)
 CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
 CWE-190
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12362>

RHSA-2021:1739 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1739>

RHSA-2021:1620 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1620>

RHSA-2021:1578 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1578>

Уязвимость

Риск: Средний

ALTX ID
357334

Red Hat/CentOS -- уязвимость в Python, python27:2.7, python3, python38:3.8 (CVE-2020-26116)

Описание

В продукте Python, python27:2.7, python3, python38:3.8 обнаружена уязвимость CVE-2020-26116.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:153696

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:153696>

RHSA-2022:5235 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:5235>

CESA-2022:5235 (CESA-2022:5235)

<http://lists.centos.org/pipermail/centos-announce/2022-August/073601.html>

RHSA-2021:3366 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3366>

BDU:2021-03738 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03738>

CVE-2020-26116 (CVE)

CVSSv2: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)
 CVSSv3: Базовая оценка 7.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N)
 CWE-116
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26116>

RHSA-2021:1633 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1633>

RHSA-2021:1761 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1761>

RHSA-2021:1879 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1879>

Уязвимость

Риск: Средний

ALTX ID
357336

Red Hat/CentOS -- уязвимость в Python, python27:2.7, python-urllib3 (CVE-2020-26137)

Описание

В продуктах Python, python27:2.7, python-urllib3 обнаружена уязвимость CVE-2020-26137.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:153698

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:153698>

RHSA-2022:5235 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:5235>

CESA-2022:5235 (CESA-2022:5235)

<http://lists.centos.org/pipermail/centos-announce/2022-August/073601.html>

BDU:2021-05230 (FSTEC)

<https://bdu.fstec.ru/vul/2021-05230>

CVE-2020-26137 (CVE)

CVSSv2: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CWE-74

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26137>

RHSA-2021:1631 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1631>

RHSA-2021:1761 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1761>

Уязвимость

Риск: Средний

ALTX ID
357386

Red Hat/CentOS -- уязвимость в Python, python27:2.7, python3, python38:3.8 (CVE-2021-3177)

Описание

В продукте Python, python27:2.7, python3, python38:3.8 обнаружена уязвимость CVE-2021-3177.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:153748

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:153748>

RHSA-2022:5235 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:5235>

CESA-2022:5235 (CESA-2022:5235)

<http://lists.centos.org/pipermail/centos-announce/2022-August/073601.html>

VULN-20220110.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220110.2.pdf>

BDU:2021-01781 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01781>

CVE-2021-3177 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-120

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3177>

RHSA-2021:1633 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1633>

RHSA-2021:1761 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1761>

RHSA-2021:1879 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:1879>

Уязвимость

Риск: Средний

ALTX ID
359154

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-12363)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-12363.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:155072

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:155072>

CESA-2021:2314 (CESA-2021:2314)

<http://lists.centos.org/pipermail/centos-announce/2021-June/048337.html>

BDU:2021-00822 (FSTEC)

<https://bdu.fstec.ru/vul/2021-00822>

CVE-2020-12363 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-20

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12363>

RHSA-2021:2316 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2316>

RHSA-2021:2314 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2314>

Уязвимость

Риск: Средний

ALTX ID
359155

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-12364)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-12364.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:155073

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:155073>

CESA-2021:2314 (CESA-2021:2314)

<http://lists.centos.org/pipermail/centos-announce/2021-June/048337.html>

BDU:2021-00823 (FSTEC)

<https://bdu.fstec.ru/vul/2021-00823>

CVE-2020-12364 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12364>

RHSA-2021:2316 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2316>

RHSA-2021:2314 (VENDOR)<https://access.redhat.com/errata/RHSA-2021:2314>**Уязвимость**

Риск: Средний

ALTX ID

359157

Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-24511)**Описание**

В продукте microcode_ctl обнаружена уязвимость CVE-2020-24511.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:155075**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:155075>**RHSA-2021:3364 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3364>**RHSA-2021:3322 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3322>**RHSA-2021:2304 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2304>**RHSA-2021:2305 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2305>**RHSA-2021:2308 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2308>**RHSA-2021:3317 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3317>**RHSA-2021:3323 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3323>**RHSA-2021:3176 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3176>**RHSA-2021:3255 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3255>**RHSA-2021:3028 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3028>**CESA-2021:3028 (CESA-2021:3028)**<http://lists.centos.org/pipermail/centos-announce/2021-August/048347.html>**RHSA-2021:3029 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3029>**RHSA-2021:3027 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3027>**BDU:2021-03385 (FSTEC)**<https://bdu.fstec.ru/vul/2021-03385>**CVE-2020-24511 (CVE)**

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)

CWE-668

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24511>**RHSA-2021:2300 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2300>**RHSA-2021:2299 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2299>

RHSA-2021:2301 (VENDOR)<https://access.redhat.com/errata/RHSA-2021:2301>**RHSA-2021:2302 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2302>**RHSA-2021:2306 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2306>**RHSA-2021:2303 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2303>**RHSA-2021:2307 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2307>

Уязвимость

Риск: Средний

ALTX ID
359160**Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-27170)****Описание**

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-27170.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:155078**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:155078>**CESA-2021:2314 (CESA-2021:2314)**<http://lists.centos.org/pipermail/centos-announce/2021-June/048337.html>**BDU:2021-01865 (FSTEC)**<https://bdu.fstec.ru/vul/2021-01865>**CVE-2020-27170 (CVE)**

CVSSv2: Базовая оценка 1.8 (AV:L/AC:M/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 4.6 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)

CWE-203

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27170>**RHSA-2021:2316 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2316>**RHSA-2021:2314 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2314>

Уязвимость

Риск: Средний

ALTX ID
361757**Red Hat/CentOS -- уязвимость в grm (CVE-2021-20271)****Описание**

В продукте grm обнаружена уязвимость CVE-2021-20271.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:156244**<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:156244>

VULN-20220719.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220719.2.pdf>

BDU:2022-00716 (FSTEC)

<https://bdu.fstec.ru/vul/2022-00716>

VULN-20220110.4 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220110.4.pdf>

RHSA-2021:4975 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4975>

RHSA-2021:4785 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4785>

CESA-2021:4785 (CESA-2021:4785)

<http://lists.centos.org/pipermail/centos-announce/2021-December/048415.html>

RHSA-2021:4771 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4771>

RHSA-2021:2791 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2791>

CVE-2021-20271 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

CWE-345

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20271>

RHSA-2021:2574 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2574>

Уязвимость

Риск: Средний

ALTX ID

364171

Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2019-20934)

Описание

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2019-20934.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:158177

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:158177>

RHSA-2021:3987 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3987>

BDU:2020-05553 (FSTEC)

<https://bdu.fstec.ru/vul/2020-05553>

CVE-2019-20934 (CVE)

CVSSv2: Базовая оценка 5.4 (AV:L/AC:M/Au:N/C:P/I:N/A:C)

CVSSv3: Базовая оценка 5.3 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20934>

RHSA-2021:2726 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2726>

RHSA-2021:2725 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2725>

CESA-2021:2725 (CESA-2021:2725)

<http://lists.centos.org/pipermail/centos-announce/2021-July/048344.html>

Уязвимость

Риск: Средний

ALTIX ID
364175**Red Hat/CentOS -- уязвимость в kpatch-patch-3_10_0-1062_36_1, kernel, kernel-rt, kpatch-patch-4_18_0-193_19_1, kpatch-patch-3_10_0-1160, kpatch-patch-3_10_0-957_61_1, kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-305 (CVE-2021-32399)****Описание**

В продукте kpatch-patch-3_10_0-1062_36_1, kernel, kernel-rt, kpatch-patch-4_18_0-193_19_1, kpatch-patch-3_10_0-1160, kpatch-patch-3_10_0-957_61_1, kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-305 обнаружена уязвимость CVE-2021-32399.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки**oval:ru.altx-soft.nix:def:158181**<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:158181>**RHSA-2021:3375 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3375>**RHSA-2022:0157 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0157>**RHSA-2021:3523 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3523>**RHSA-2021:3522 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3522>**RHSA-2021:3725 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3725>**RHSA-2021:3328 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3328>**RHSA-2021:3363 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3363>**RHSA-2021:3380 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3380>**RHSA-2021:3381 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3381>**RHSA-2021:3392 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3392>**RHSA-2021:3399 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3399>**RHSA-2021:3327 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3327>**CESA-2021:3327 (CESA-2021:3327)**<http://lists.centos.org/pipermail/centos-announce/2021-August/060904.html>**RHSA-2021:3320 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3320>**RHSA-2021:3321 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3321>**BDU:2021-04838 (FSTEC)**<https://bdu.fstec.ru/vul/2021-04838>**RHSA-2021:3181 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3181>**RHSA-2021:3173 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3173>

CVE-2021-32399 (CVE)

CVSSv2: Базовая оценка 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-362

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32399>**RHSA-2021:2716 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2716>**RHSA-2021:2715 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2715>**RHSA-2021:2714 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:2714>

Уязвимость

Риск: Средний

ALTX ID
365758**Red Hat/CentOS -- уязвимость в kernel, kernel-rt, kpatch-patch-3_10_0-1062_40_1, kpatch-patch-3_10_0-1160_11_1, kpatch-patch-3_10_0-957_61_1, kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-193_19_1, kpatch-patch-4_18_0-305 (CVE-2021-22543)****Описание**

В продукте kernel, kernel-rt, kpatch-patch-3_10_0-1062_40_1, kpatch-patch-3_10_0-1160_11_1, kpatch-patch-3_10_0-957_61_1, kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-193_19_1, kpatch-patch-4_18_0-305 обнаружена уязвимость CVE-2021-22543.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:159350

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:159350>**RHSA-2021:3375 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3375>**RHSA-2022:5640 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:5640>**RHSA-2021:3767 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3767>**RHSA-2021:3725 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3725>**RHSA-2021:3766 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3766>**RHSA-2021:3768 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3768>**RHSA-2021:3801 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3801>**CESA-2021:3801 (CESA-2021:3801)**<http://lists.centos.org/pipermail/centos-announce/2021-November/060946.html>**RHSA-2021:3802 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3802>**RHSA-2021:3812 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3812>**RHSA-2021:3814 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3814>**RHSA-2021:3363 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3363>**RHSA-2021:3380 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3380>

RHSA-2021:3987 (VENDOR)<https://access.redhat.com/errata/RHSA-2021:3987>**RHSA-2021:4000 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:4000>**BDU:2021-04854 (FSTEC)**<https://bdu.fstec.ru/vul/2021-04854>**RHSA-2021:3181 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3181>**RHSA-2021:3173 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3173>**CVE-2021-22543 (CVE)**

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-119

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22543>**RHSA-2021:3057 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3057>**RHSA-2021:3088 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3088>**RHSA-2021:3044 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:3044>

Уязвимость

Риск: Средний

ALTX ID

370703

Red Hat/CentOS -- уязвимость в kernel, kernel-rt, kpatch-patch-3_10_0-1062_43_1, kpatch-patch-3_10_0-1160_11_1, kpatch-patch-3_10_0-957_65_1, kpatch-patch-4_18_0-147_34_1, kpatch-patch-4_18_0-193_37_1, kpatch-patch-4_18_0-305 (CVE-2020-36385)

Описание

В продукте kernel, kernel-rt, kpatch-patch-3_10_0-1062_43_1, kpatch-patch-3_10_0-1160_11_1, kpatch-patch-3_10_0-957_65_1, kpatch-patch-4_18_0-147_34_1, kpatch-patch-4_18_0-193_37_1, kpatch-patch-4_18_0-305 обнаружена уязвимость CVE-2020-36385.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:162858

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:162858>**RHSA-2021:4875 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:4875>**BDU:2022-05916 (FSTEC)**<https://bdu.fstec.ru/vul/2022-05916>**VULN-20220719.2 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220719.2.pdf>**RHSA-2022:0157 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0157>**RHSA-2021:4971 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:4971>**CESA-2021:4777 (CESA-2021:4777)**<http://lists.centos.org/pipermail/centos-announce/2021-December/048420.html>**RHSA-2021:4871 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:4871>**RHSA-2021:4859 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:4859>

- RHSA-2021:4770 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4770>
- RHSA-2021:4768 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4768>
- RHSA-2021:4798 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4798>
- RHSA-2021:4779 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4779>
- RHSA-2021:4777 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4777>
- RHSA-2021:4774 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4774>
- RHSA-2021:4773 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4773>
- RHSA-2021:4692 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4692>
- RHSA-2021:4687 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4687>
- RHSA-2021:4088 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4088>
- RHSA-2021:4122 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4122>
- RHSA-2021:4597 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4597>
- RHSA-2021:4056 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4056>
- CVE-2020-36385 (CVE)**
CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
CWE-416
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36385>
- RHSA-2021:3987 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3987>

Уязвимость	Риск: Средний
ALTX ID	Red Hat/CentOS -- уязвимость в kernel (CVE-2020-27777)
371408	
Описание	

В продукте kernel обнаружена уязвимость CVE-2020-27777.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

- oval:ru.altx-soft.nix:def:163398**
<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:163398>
- RHSA-2021:3327 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3327>
- CESA-2021:3327 (CESA-2021:3327)**
<http://lists.centos.org/pipermail/centos-announce/2021-August/060904.html>
- BDU:2021-03443 (FSTEC)**
<https://bdu.fstec.ru/vul/2021-03443>

CVE-2020-27777 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
CVSSv3: Базовая оценка 6.6 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)
CWE-862
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27777>

RHSA-2021:4356 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4356>

Уязвимость	Риск: Средний
ALTX ID 371448	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2021-29650)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2021-29650.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:163438
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:163438>

RHSA-2021:3328 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:3328>

RHSA-2021:3327 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:3327>

CESA-2021:3327 (CESA-2021:3327)
<http://lists.centos.org/pipermail/centos-announce/2021-August/060904.html>

BDU:2021-02100 (FSTEC)
<https://bdu.fstec.ru/vul/2021-02100>

CVE-2021-29650 (CVE)
CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)
CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)
NVD-CWE-noinfo
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29650>

RHSA-2021:4140 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4140>

RHSA-2021:4356 (VENDOR)
<https://access.redhat.com/errata/RHSA-2021:4356>

Уязвимость	Риск: Средний
ALTX ID 371460	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2021-3564)
Описание	

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2021-3564.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:163450
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:163450>

CESA-2022:0620 (CESA-2022:0620)

<http://lists.centos.org/pipermail/centos-announce/2022-February/073573.html>

RHSA-2022:0620 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0620>

RHSA-2022:0622 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0622>

BDU:2021-04862 (FSTEC)

<https://bdu.fstec.ru/vul/2021-04862>

CVE-2021-3564 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)

CWE-415

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3564>

RHSA-2021:4140 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4140>

RHSA-2021:4356 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4356>

Уязвимость

Риск: Средний

ALTX ID
371461

Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2021-3573)

Описание

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2021-3573.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:163451

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:163451>

CESA-2022:0620 (CESA-2022:0620)

<http://lists.centos.org/pipermail/centos-announce/2022-February/073573.html>

RHSA-2022:0620 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0620>

RHSA-2022:0622 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0622>

BDU:2021-04846 (FSTEC)

<https://bdu.fstec.ru/vul/2021-04846>

CVE-2021-3573 (CVE)

CVSSv2: Базовая оценка 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 6.4 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)

CWE-362

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3573>

RHSA-2021:4140 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4140>

RHSA-2021:4356 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4356>

Уязвимость

Риск: Средний

ALTX ID
372328

Red Hat/CentOS -- уязвимость в OpenSSL, edk2 (CVE-2021-23840)

Описание

В продуктах OpenSSL, edk2 обнаружена уязвимость CVE-2021-23840.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:164142

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:164142>

VULN-20221021.3 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221021.3.pdf>

VULN-20220901.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220901.5.pdf>

VULN-20220719.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220719.2.pdf>

RHSA-2021:3798 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3798>

CESA-2021:3798 (CESA-2021:3798)

<http://lists.centos.org/pipermail/centos-announce/2021-November/060932.html>

VULN-20220110.2 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220110.2.pdf>

BDU:2021-03742 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03742>

CVE-2021-23840 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23840>

RHSA-2021:4198 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4198>

RHSA-2021:4424 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4424>

Уязвимость

Риск: Средний

ALTX ID

372329

Red Hat/CentOS -- уязвимость в OpenSSL, edk2 (CVE-2021-23841)

Описание

В продуктах OpenSSL, edk2 обнаружена уязвимость CVE-2021-23841.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:164143

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:164143>

RHSA-2021:3798 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3798>

CESA-2021:3798 (CESA-2021:3798)

<http://lists.centos.org/pipermail/centos-announce/2021-November/060932.html>

BDU:2021-03744 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03744>

CVE-2021-23841 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CVSSv3: Базовая оценка 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-476
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23841>

RHSA-2021:4198 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4198>

RHSA-2021:4424 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4424>

Уязвимость	Риск: Средний
ALTX ID 372330	Red Hat/CentOS -- уязвимость в Bind (CVE-2021-25214)
Описание	

В продукте Bind обнаружена уязвимость CVE-2021-25214.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

- oval:ru.altx-soft.nix:def:164144
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:164144>
- RHSA-2021:3325 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3325>
- CESA-2021:3325 (CESA-2021:3325)**
<http://lists.centos.org/pipermail/centos-announce/2021-September/060909.html>
- BDU:2021-02777 (FSTEC)**
<https://bdu.fstec.ru/vul/2021-02777>
- CVE-2021-25214 (CVE)**
CVSSv2: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)
CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)
CWE-617
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25214>
- RHSA-2021:4384 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:4384>

Уязвимость	Риск: Средний
ALTX ID 372919	Red Hat/CentOS -- уязвимость в krb5 (CVE-2021-37750)
Описание	

В продукте krb5 обнаружена уязвимость CVE-2021-37750.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

- oval:ru.altx-soft.nix:def:164599
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:164599>
- RHSA-2021:3576 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3576>

CVE-2021-37750 (CVE)

CVSSv2: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:N/I:N/A:P)
 CVSSv3: Базовая оценка 6.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)
 CWE-476
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37750>

RHSA-2021:4788 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4788>

CESA-2021:4788 (CESA-2021:4788)

<http://lists.centos.org/pipermail/centos-announce/2021-December/048422.html>

Уязвимость

Риск: Средний

ALTX ID
372920

Red Hat/CentOS -- уязвимость в openssh (CVE-2021-41617)**Описание**

В продукте openssh обнаружена уязвимость CVE-2021-41617.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:164600

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:164600>

RHSA-2022:2013 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:2013>

CVE-2021-41617 (CVE)

CVSSv2: Базовая оценка 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)
 CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
 NVD-CWE-Other
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41617>

RHSA-2021:4782 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:4782>

CESA-2021:4782 (CESA-2021:4782)

<http://lists.centos.org/pipermail/centos-announce/2021-December/048411.html>

Уязвимость

Риск: Средний

ALTX ID
378482

Red Hat/CentOS -- уязвимость в libxml2 (CVE-2016-4658)**Описание**

В продукте libxml2 обнаружена уязвимость CVE-2016-4658.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:168631

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:168631>

BDU:2021-03125 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03125>

CVE-2016-4658 (CVE)

CVSSv2: Базовая оценка 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
 CVSSv3: Базовая оценка 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
 CWE-119
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4658>

RHSA-2021:3810 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3810>

CESA-2021:3810 (CESA-2021:3810)

<http://lists.centos.org/pipermail/centos-announce/2021-November/060926.html>

Уязвимость	Риск: Средний
ALTX ID 378736	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2021-29154)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2021-29154.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

- oval:ru.altx-soft.nix:def:168885**
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:168885>
- RHSA-2022:1988 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:1988>
- RHSA-2022:1975 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:1975>
- BDU:2021-02182 (FSTEC)**
<https://bdu.fstec.ru/vul/2021-02182>
- CVE-2021-29154 (CVE)**
 CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
 CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
 CWE-77
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29154>
- RHSA-2021:3328 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3328>
- RHSA-2021:3327 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2021:3327>
- CESA-2021:3327 (CESA-2021:3327)**
<http://lists.centos.org/pipermail/centos-announce/2021-August/060904.html>

Уязвимость	Риск: Средний
ALTX ID 378750	Red Hat/CentOS -- уязвимость в kpatch-patch-3_10_0-957_84_1, kernel, kernel-rt, kpatch-patch-3_10_0-1160, kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-193_19_1 (CVE-2021-3715)
Описание	

В продукте kpatch-patch-3_10_0-957_84_1, kernel, kernel-rt, kpatch-patch-3_10_0-1160, kpatch-patch-4_18_0-147_27_1, kpatch-patch-4_18_0-193_19_1 обнаружена уязвимость CVE-2021-3715.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:168899

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:168899>

RHSA-2021:3445 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3445>

RHSA-2022:7173 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7173>

BDU:2022-03144 (FSTEC)

<https://bdu.fstec.ru/vul/2022-03144>

CVE-2021-3715 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3715>

RHSA-2021:3442 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3442>

RHSA-2021:3443 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3443>

RHSA-2021:3444 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3444>

RHSA-2021:3446 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3446>

RHSA-2021:3441 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3441>

RHSA-2021:3439 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3439>

RHSA-2021:3438 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3438>

CESA-2021:3438 (CESA-2021:3438)

<http://lists.centos.org/pipermail/centos-announce/2021-September/060915.html>

Уязвимость

Риск: Средний

ALTX ID
379780

Red Hat/CentOS -- уязвимость в httpd:2.4, httpd (CVE-2021-34798)

Описание

В продуктах httpd:2.4, httpd обнаружена уязвимость CVE-2021-34798.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:169467

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:169467>

VULN-20220914.14 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220914.14.pdf>

VULN-20220426.6 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220426.6.pdf>

VULN-20220426.1 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220426.1.pdf>

RHSA-2022:0891 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0891>

BDU:2021-05873 (FSTEC)

<https://bdu.fstec.ru/vul/2021-05873>

CESA-2022:0143 (CESA-2022:0143)

<http://lists.centos.org/pipermail/centos-announce/2022-January/073551.html>

CVE-2021-34798 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34798>

RHSA-2022:0143 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0143>

Уязвимость	Риск: Средний
ALT X ID	Red Hat/CentOS -- уязвимость в kernel-rt, kernel, kpatch-patch-4_18_0-147_43_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_46_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_70_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 (CVE-2021-4155)
379792	

Описание

В продукте kernel-rt, kernel, kpatch-patch-4_18_0-147_43_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_46_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_70_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 обнаружена уязвимость CVE-2021-4155.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:169479

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:169479>

RHSA-2022:0187 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0187>

RHSA-2022:0344 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0344>

RHSA-2022:0335 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0335>

RHSA-2022:0629 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0629>

RHSA-2022:0958 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0958>

RHSA-2022:0712 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0712>

RHSA-2022:1417 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1417>

CESA-2022:0620 (CESA-2022:0620)

<http://lists.centos.org/pipermail/centos-announce/2022-February/073573.html>

RHSA-2022:0718 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0718>

RHSA-2022:0590 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0590>

RHSA-2022:0592 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0592>

RHSA-2022:0620 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0620>

RHSA-2022:0622 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0622>

RHSA-2022:0636 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0636>

BDU:2022-00755 (FSTEC)

<https://bdu.fstec.ru/vul/2022-00755>

RHSA-2022:0529 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0529>

RHSA-2022:0530 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0530>

RHSA-2022:0531 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0531>

RHSA-2022:0533 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0533>

RHSA-2022:0231 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0231>

RHSA-2022:0232 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0232>

RHSA-2022:0188 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0188>

CVE-2021-4155 (CVE)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CWE-131

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4155>

RHSA-2022:0176 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0176>

RHSA-2022:0186 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0186>

Уязвимость

Риск: Средний

ALTX ID
382832

Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2020-0465)

Описание

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2020-0465.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:171401

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:171401>

CESA-2022:0620 (CESA-2022:0620)

<http://lists.centos.org/pipermail/centos-announce/2022-February/073573.html>

CVE-2020-0465 (CVE)

CVSSv2: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 6.8 (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-787

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0465>

RHSA-2022:0620 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0620>

RHSA-2022:0622 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0622>

Уязвимость

Риск: Средний

ALTX ID

382834

Red Hat/CentOS -- уязвимость в openldap (CVE-2020-25709)

Описание

В продукте openldap обнаружена уязвимость CVE-2020-25709.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:171403

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:171403>

VULN-20220727.12 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.12.pdf>

CESA-2022:0621 (CESA-2022:0621)

<http://lists.centos.org/pipermail/centos-announce/2022-February/073566.html>

BDU:2022-00231 (FSTEC)

<https://bdu.fstec.ru/vul/2022-00231>

CVE-2020-25709 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-617

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25709>

RHSA-2022:0621 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0621>

Уязвимость

Риск: Средний

ALTX ID

382835

Red Hat/CentOS -- уязвимость в openldap (CVE-2020-25710)

Описание

В продукте openldap обнаружена уязвимость CVE-2020-25710.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:171404

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:171404>

VULN-20220727.12 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.12.pdf>

CESA-2022:0621 (CESA-2022:0621)

<http://lists.centos.org/pipermail/centos-announce/2022-February/073566.html>

BDU:2022-00230 (FSTEC)

<https://bdu.fstec.ru/vul/2022-00230>

CVE-2020-25710 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-617

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25710>

RHSA-2022:0621 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0621>

Уязвимость

Риск: Средний

ALTX ID
382838

Red Hat/CentOS -- уязвимость в kernel-rt, kernel, kpatch-patch-4_18_0-147_44_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_49_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_72_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 (CVE-2021-0920)

Описание

В продукте kernel-rt, kernel, kpatch-patch-4_18_0-147_44_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_49_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_72_1, kpatch-patch-4_18_0-193_46_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 обнаружена уязвимость CVE-2021-0920.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:171407

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:171407>

RHSA-2022:0629 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0629>

RHSA-2022:0771 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0771>

RHSA-2022:0823 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0823>

RHSA-2022:0851 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0851>

RHSA-2022:0958 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0958>

RHSA-2022:0819 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0819>

RHSA-2022:1417 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1417>

RHSA-2022:1324 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1324>

RHSA-2022:1373 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1373>

RHSA-2022:1103 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1103>

RHSA-2022:1104 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1104>

RHSA-2022:1106 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1106>

RHSA-2022:1107 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1107>

RHSA-2022:0825 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0825>

RHSA-2022:0849 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0849>

RHSA-2022:0772 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0772>

RHSA-2022:0777 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0777>

CESA-2022:0620 (CESA-2022:0620)

<http://lists.centos.org/pipermail/centos-announce/2022-February/073573.html>

BDU:2022-00836 (FSTEC)<https://bdu.fstec.ru/vul/2022-00836>**CVE-2021-0920 (CVE)**

CVSSv2: Базовая оценка 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 6.4 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)

CWE-362

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-0920>**RHSA-2022:0590 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0590>**RHSA-2022:0592 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0592>**RHSA-2022:0620 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0620>**RHSA-2022:0622 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0622>**RHSA-2022:0636 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0636>

Уязвимость

Риск: Средний

ALT X ID
382887**Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2021-3752)**

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2021-3752.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:171456<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:171456>**RHSA-2022:1988 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1988>**RHSA-2022:1975 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1975>**CESA-2022:0620 (CESA-2022:0620)**<http://lists.centos.org/pipermail/centos-announce/2022-February/073573.html>**BDU:2021-04803 (FSTEC)**<https://bdu.fstec.ru/vul/2021-04803>**CVE-2021-3752 (CVE)**

CVSSv2: Базовая оценка 7.9 (AV:A/AC:M/Au:N/C:C/I:C/A:C)

CVSSv3: Базовая оценка 7.0 (CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3752>**RHSA-2022:0620 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0620>**RHSA-2022:0622 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0622>

Уязвимость

Риск: Средний

ALT X ID
382890**Red Hat/CentOS -- уязвимость в kernel-rt, kernel, kpatch-patch-4_18_0-147_44_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_46_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_72_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 (CVE-2022-0330)**

Описание

В продукте kernel-rt, kernel, kpatch-patch-4_18_0-147_44_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_46_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_72_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 обнаружена уязвимость CVE-2022-0330.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:171459

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:171459>

RHSA-2022:0771 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0771>

RHSA-2022:0821 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0821>

RHSA-2022:0823 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0823>

RHSA-2022:0851 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0851>

RHSA-2022:0958 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0958>

BDU:2022-05890 (FSTEC)

<https://bdu.fstec.ru/vul/2022-05890>

RHSA-2022:0819 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0819>

RHSA-2022:0712 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0712>

VULN-20220412.4 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220412.4.pdf>

RHSA-2022:1103 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1103>

RHSA-2022:1104 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1104>

RHSA-2022:1106 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1106>

RHSA-2022:1107 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1107>

VULN-20220318.3 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220318.3.pdf>

RHSA-2022:0825 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0825>

RHSA-2022:0849 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0849>

RHSA-2022:0925 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0925>

RHSA-2022:0772 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0772>

RHSA-2022:0777 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0777>

RHSA-2022:0820 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0820>

CESA-2022:0620 (CESA-2022:0620)

<http://lists.centos.org/pipermail/centos-announce/2022-February/073573.html>

RHSA-2022:0718 (VENDOR)<https://access.redhat.com/errata/RHSA-2022:0718>**CVE-2022-0330 (CVE)**

CVSSv2: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-281

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0330>**RHSA-2022:0592 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0592>**RHSA-2022:0620 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0620>**RHSA-2022:0622 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0622>

Уязвимость

Риск: Средний

ALTX ID

382893

Red Hat/CentOS -- уязвимость в kernel-rt, kernel, kpatch-patch-4_18_0-147_44_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_49_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_72_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 (CVE-2022-22942)

Описание

В продукте kernel-rt, kernel, kpatch-patch-4_18_0-147_44_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_49_1, kpatch-patch-3_10_0-1160_21_1, kpatch-patch-3_10_0-957_72_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 обнаружена уязвимость CVE-2022-22942.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:171462

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:171462>**RHSA-2022:0771 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0771>**RHSA-2022:0821 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0821>**RHSA-2022:0823 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0823>**RHSA-2022:0851 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0851>**RHSA-2022:0958 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0958>**RHSA-2022:0819 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:0819>**RHSA-2022:1324 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1324>**RHSA-2022:1373 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1373>**VULN-20220412.4 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220412.4.pdf>**RHSA-2022:1103 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1103>**RHSA-2022:1107 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:1107>**VULN-20220318.3 (NKCKI)**<https://safe-surf.ru/upload/VULN/VULN-20220318.3.pdf>

RHSA-2022:0825 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0825>

RHSA-2022:0849 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0849>

RHSA-2022:0925 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0925>

RHSA-2022:0772 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0772>

RHSA-2022:0777 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0777>

RHSA-2022:0820 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0820>

CESA-2022:0620 (CESA-2022:0620)

<http://lists.centos.org/pipermail/centos-announce/2022-February/073573.html>

BDU:2022-00607 (FSTEC)

<https://bdu.fstec.ru/vul/2022-00607>

CVE-2022-22942 (CVE)

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22942>

RHSA-2022:0592 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0592>

RHSA-2022:0620 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0620>

RHSA-2022:0622 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0622>

Уязвимость

Риск: Средний

ALT X ID
383728

Red Hat/CentOS -- уязвимость в kernel-rt, kernel, kpatch-patch-4_18_0-147_44_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_51_1, kpatch-patch-3_10_0-1160_31_1, kpatch-patch-3_10_0-957_72_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 (CVE-2022-0492)

Описание

В продукте kernel-rt, kernel, kpatch-patch-4_18_0-147_44_1, kpatch-patch-4_18_0-147_58_1, kpatch-patch-3_10_0-1062_51_1, kpatch-patch-3_10_0-1160_31_1, kpatch-patch-3_10_0-957_72_1, kpatch-patch-4_18_0-193_47_1, kpatch-patch-4_18_0-305, kpatch-patch-4_18_0-348 обнаружена уязвимость CVE-2022-0492.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:172033

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:172033>

RHSA-2022:0821 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0821>

RHSA-2022:0823 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0823>

RHSA-2022:0851 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0851>

RHSA-2022:0958 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:0958>

RHSA-2022:1413 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1413>

RHSA-2022:5157 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:5157>

- RHSA-2022:4717 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:4717>
- RHSA-2022:4721 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:4721>
- RHSA-2022:4655 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:4655>
- RHSA-2022:4644 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:4644>
- RHSA-2022:4642 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:4642>
- CESA-2022:4642 (CESA-2022:4642)**
<http://lists.centos.org/pipermail/centos-announce/2022-May/073587.html>
- RHSA-2022:2186 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:2186>
- RHSA-2022:2189 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:2189>
- RHSA-2022:2211 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:2211>
- RHSA-2022:1455 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:1455>
- RHSA-2022:0819 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:0819>
- RHSA-2022:1418 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:1418>
- RHSA-2022:1417 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:1417>
- RHSA-2022:0825 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:0825>
- RHSA-2022:0849 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:0849>
- RHSA-2022:0925 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:0925>
- BDU:2022-00737 (FSTEC)**
<https://bdu.fstec.ru/vul/2022-00737>
- CVE-2022-0492 (CVE)**
CVSSv2: Базовая оценка 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)
CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CWE-287
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0492>
- RHSA-2022:0820 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:0820>

Уязвимость	Риск: Средний
ALTX ID	Red Hat/CentOS -- уязвимость в httpd:2.4, httpd (CVE-2022-22720)
385532	
Описание	
В продуктах httpd:2.4, httpd обнаружена уязвимость CVE-2022-22720.	
Исправление	
Необходимо установить актуальное обновление от производителя.	
Ссылки	

oval:ru.altx-soft.nix:def:173593

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:173593>

RHSA-2022:1080 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1080>

RHSA-2022:1173 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1173>

VULN-20221005.11 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.11.pdf>

VULN-20221005.10 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.10.pdf>

CESA-2022:1045 (CESA-2022:1045)

<http://lists.centos.org/pipermail/centos-announce/2022-March/073576.html>

RHSA-2022:1072 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1072>

RHSA-2022:1102 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1102>

RHSA-2022:1136 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1136>

RHSA-2022:1137 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1137>

RHSA-2022:1138 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1138>

RHSA-2022:1139 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1139>

BDU:2022-01456 (FSTEC)

<https://bdu.fstec.ru/vul/2022-01456>

CVE-2022-22720 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-444

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22720>

RHSA-2022:1045 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1045>

RHSA-2022:1049 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1049>

Уязвимость

Риск: Средний

ALTX ID

390407

Red Hat/CentOS -- уязвимость в gzip, xz (CVE-2022-1271)

Описание

В продуктах gzip, xz обнаружена уязвимость CVE-2022-1271.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:177577

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:177577>

RHSA-2022:1592 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1592>

RHSA-2022:4994 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:4994>

RHSA-2022:4582 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:4582>

RHSA-2022:4940 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:4940>

VULN-20221005.9 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.9.pdf>

VULN-20221005.8 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.8.pdf>

VULN-20220727.7 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.7.pdf>

VULN-20220727.17 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220727.17.pdf>

VULN-20220624.8 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220624.8.pdf>

VULN-20220624.3 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220624.3.pdf>

RHSA-2022:4993 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:4993>

RHSA-2022:5052 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:5052>

VULN-20220602.1 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20220602.1.pdf>

CESA-2022:2191 (CESA-2022:2191)

<http://lists.centos.org/pipermail/centos-announce/2022-May/073585.html>

RHSA-2022:2191 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:2191>

RHSA-2022:1665 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1665>

RHSA-2022:1676 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1676>

BDU:2022-02113 (FSTEC)

<https://bdu.fstec.ru/vul/2022-02113>

CVE-2022-1271 (CVE)

CVSSv3: Базовая оценка 8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-20

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1271>

RHSA-2022:1537 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1537>

Уязвимость	Риск: Средний
ALTX ID 394103	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2021-26401)
Описание	

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2021-26401.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:180797

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:180797>

CESA-2023:0399 (CESA-2023:0399)

<http://lists.centos.org/pipermail/centos-announce/2023-January/086370.html>

RHSA-2023:0400 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0400>

RHSA-2023:0399 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0399>

RHSA-2023:0187 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0187>

BDU:2022-03555 (FSTEC)

<https://bdu.fstec.ru/vul/2022-03555>

RHSA-2022:1988 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1988>

CVE-2021-26401 (CVE)

CVSSv2: Базовая оценка 1.8 (AV:L/AC:M/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26401>

RHSA-2022:1975 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:1975>

Уязвимость	Риск: Средний
ALTX ID 403314	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2022-21123)
Описание	

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2022-21123.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:186999

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:186999>

RHSA-2022:6872 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6872>

RHSA-2022:6991 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6991>

RHSA-2022:7280 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7280>

RHSA-2022:8974 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8974>

RHSA-2022:8973 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8973>

RHSA-2022:6460 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6460>

RHSA-2022:7933 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7933>

RHSA-2022:8267 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8267>

RHSA-2022:7279 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7279>

RHSA-2022:6983 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6983>

RHSA-2022:6437 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6437>

CESA-2022:5937 (CESA-2022:5937)

<http://lists.centos.org/pipermail/centos-announce/2022-August/073632.html>

BDU:2022-03532 (FSTEC)

<https://bdu.fstec.ru/vul/2022-03532>

CVE-2022-21123 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CWE-459

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21123>

RHSA-2022:5939 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:5939>

RHSA-2022:5937 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:5937>

Уязвимость	Риск: Средний
ALTX ID 403315	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2022-21125)
Описание	

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2022-21125.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:187000

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:187000>

RHSA-2022:6872 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6872>

RHSA-2022:6991 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6991>

RHSA-2022:7280 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7280>

RHSA-2022:8974 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8974>

RHSA-2022:8973 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8973>

RHSA-2022:6460 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6460>

RHSA-2022:7933 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7933>

RHSA-2022:8267 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8267>

RHSA-2022:7279 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7279>

RHSA-2022:6983 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6983>

RHSA-2022:6437 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6437>

CESA-2022:5937 (CESA-2022:5937)

<http://lists.centos.org/pipermail/centos-announce/2022-August/073632.html>

BDU:2022-05155 (FSTEC)

<https://bdu.fstec.ru/vul/2022-05155>

CVE-2022-21125 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)

CWE-459

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21125>

RHSA-2022:5939 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:5939>

RHSA-2022:5937 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:5937>

Уязвимость	Риск: Средний
ALTX ID 403316	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2022-21166)
Описание	

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2022-21166.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:187001

<https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:187001>

RHSA-2022:6872 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6872>

RHSA-2022:6991 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6991>

RHSA-2022:7280 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7280>

RHSA-2022:8974 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8974>

RHSA-2022:8973 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8973>

RHSA-2022:6460 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6460>

RHSA-2022:7933 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7933>

RHSA-2022:8267 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:8267>

RHSA-2022:7279 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:7279>

RHSA-2022:6983 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6983>

RHSA-2022:6437 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6437>

CESA-2022:5937 (CESA-2022:5937)

<http://lists.centos.org/pipermail/centos-announce/2022-August/073632.html>

BDU:2022-03600 (FSTEC)

<https://bdu.fstec.ru/vul/2022-03600>

CVE-2022-21166 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)
 CVSSv3: Базовая оценка 5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)
 CWE-459
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21166>

RHSA-2022:5939 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:5939>

RHSA-2022:5937 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:5937>

Уязвимость	Риск: Средний
ALTX ID 405345	Red Hat/CentOS -- уязвимость в open-vm-tools (CVE-2022-31676)
Описание	

В продукте open-vm-tools обнаружена уязвимость CVE-2022-31676.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

- oval:ru.altx-soft.nix:def:188524**
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:188524>
- RHSA-2022:6354 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:6354>
- VULN-20221213.3 (NKCKI)**
<https://safe-surf.ru/upload/VULN/VULN-20221213.3.pdf>
- RHSA-2022:6358 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:6358>
- CESA-2022:6381 (CESA-2022:6381)**
<http://lists.centos.org/pipermail/centos-announce/2022-September/073638.html>
- BDU:2022-05274 (FSTEC)**
<https://bdu.fstec.ru/vul/2022-05274>
- CVE-2022-31676 (CVE)**
 CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
 CWE-269
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31676>
- RHSA-2022:6357 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:6357>
- RHSA-2022:6355 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:6355>
- RHSA-2022:6356 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:6356>
- RHSA-2022:6381 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2022:6381>

Уязвимость	Риск: Средний
ALTX ID 410364	Red Hat/CentOS -- уязвимость в Bind, bind9.16 (CVE-2022-38177)
Описание	

В продуктах Bind, bind9.16 обнаружена уязвимость CVE-2022-38177.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:192790

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:192790>

RHSA-2022:6764 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6764>

CESA-2022:6765 (CESA-2022:6765)

<http://lists.centos.org/pipermail/centos-announce/2022-October/073648.html>

BDU:2022-06120 (FSTEC)

<https://bdu.fstec.ru/vul/2022-06120>

CVE-2022-38177 (CVE)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-347

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38177>

RHSA-2022:6763 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6763>

RHSA-2022:6765 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6765>

RHSA-2022:6778 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6778>

RHSA-2022:6779 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6779>

RHSA-2022:6780 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6780>

RHSA-2022:6781 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6781>

Уязвимость

Риск: Средний

ALTX ID
410365

Red Hat/CentOS -- уязвимость в Bind, bind9.16 (CVE-2022-38178)

Описание

В продуктах Bind, bind9.16 обнаружена уязвимость CVE-2022-38178.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:192791

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:192791>

RHSA-2022:6764 (VENDOR)

<https://access.redhat.com/errata/RHSA-2022:6764>

CESA-2022:6765 (CESA-2022:6765)

<http://lists.centos.org/pipermail/centos-announce/2022-October/073648.html>

BDU:2022-06121 (FSTEC)

<https://bdu.fstec.ru/vul/2022-06121>

CVE-2022-38178 (CVE)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-347

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38178>

RHSA-2022:6763 (VENDOR)<https://access.redhat.com/errata/RHSA-2022:6763>**RHSA-2022:6765 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:6765>**RHSA-2022:6778 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:6778>**RHSA-2022:6779 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:6779>**RHSA-2022:6780 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:6780>**RHSA-2022:6781 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:6781>

Уязвимость

Риск: Средний

ALTX ID

412624

Red Hat/CentOS -- уязвимость в Bind, bind9.16, DHCP (CVE-2021-25220)

Описание

В продуктах Bind, bind9.16, DHCP обнаружена уязвимость CVE-2021-25220.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:194538<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:194538>**CESA-2023:0402 (CESA-2023:0402)**<http://lists.centos.org/pipermail/centos-announce/2023-January/086358.html>**RHSA-2023:0402 (VENDOR)**<https://access.redhat.com/errata/RHSA-2023:0402>**RHSA-2022:7643 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:7643>**RHSA-2022:8385 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:8385>**RHSA-2022:8068 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:8068>**BDU:2022-05754 (FSTEC)**<https://bdu.fstec.ru/vul/2022-05754>**CVE-2021-25220 (CVE)**

CVSSv2: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:N/I:P/A:N)

CVSSv3: Базовая оценка 6.8 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N)

CWE-444

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25220>**RHSA-2022:7790 (VENDOR)**<https://access.redhat.com/errata/RHSA-2022:7790>

Уязвимость

Риск: Средний

ALTX ID

418857

Red Hat/CentOS -- уязвимость в kernel-rt, kpatch-patch-5_14_0-70_17_1, kpatch-patch-4_18_0-147_70_1, kernel, kpatch-patch-3_10_0-1160_71_1, kpatch-patch-4_18_0-193_87_1, kpatch-patch-4_18_0-425_3_1, kpatch-patch-5_14_0-162_6_1 (CVE-2022-2964)

Описание

В продукте kernel-rt, kpatch-patch-5_14_0-70_17_1, kpatch-patch-4_18_0-147_70_1, kernel, kpatch-patch-3_10_0-1160_71_1,

kpatch-patch-4_18_0-193_87_1, kpatch-patch-4_18_0-425_3_1, kpatch-patch-5_14_0-162_6_1 обнаружена уязвимость CVE-2022-2964.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:199818

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:199818>

RHSA-2023:0858 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0858>

RHSA-2023:0856 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0856>

RHSA-2023:0300 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0300>

CESA-2023:0399 (CESA-2023:0399)

<http://lists.centos.org/pipermail/centos-announce/2023-January/086370.html>

RHSA-2023:0526 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0526>

RHSA-2023:0536 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0536>

RHSA-2023:0404 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0404>

RHSA-2023:0400 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0400>

RHSA-2023:0399 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0399>

RHSA-2023:0396 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0396>

RHSA-2023:0395 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0395>

RHSA-2023:0392 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0392>

RHSA-2023:0348 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0348>

RHSA-2023:0334 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0334>

RHSA-2023:0101 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0101>

BDU:2022-05848 (FSTEC)

<https://bdu.fstec.ru/vul/2022-05848>

CVE-2022-2964 (CVE)

CVSSv3: Базовая оценка 7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CWE-119

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2964>

RHSA-2023:0123 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0123>

RHSA-2023:0114 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0114>

Уязвимость

Риск: Средний

ALT X ID
419822

Red Hat/CentOS -- уязвимость в Bind (CVE-2022-2795)

Описание

В продукте Bind обнаружена уязвимость CVE-2022-2795.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:200599

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:200599>

CESA-2023:0402 (CESA-2023:0402)

<http://lists.centos.org/pipermail/centos-announce/2023-January/086358.html>

BDU:2022-06124 (FSTEC)

<https://bdu.fstec.ru/vul/2022-06124>

CVE-2022-2795 (CVE)

CVSSv3: Базовая оценка 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-400

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2795>

RHSA-2023:0402 (VENDOR)

<https://access.redhat.com/errata/RHSA-2023:0402>

Уязвимость

Риск: Низкий

ALTX ID
288302

Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2019-11727)

Описание

В продуктах nspr, nss обнаружена уязвимость CVE-2019-11727.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:104415

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:104415>

CESA-2020:4076-CentOS 7 (CESA-2020:4076)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-November/012876.html>

RHSA-2020:4076 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4076>

BDU:2020-00597 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00597>

CVE-2019-11727 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 3.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N)

CWE-295

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11727>

RHSA-2019:1951 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:1951>

Уязвимость

Риск: Низкий

ALTX ID
307171

Red Hat/CentOS -- уязвимость в gettext, emacs-gettext (CVE-2018-18751)

Описание

В продуктах gettext, emacs-gettext обнаружена уязвимость CVE-2018-18751.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:120756

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:120756>

VULN-20221005.5 (NKCKI)

<https://safe-surf.ru/upload/VULN/VULN-20221005.5.pdf>

CESA-2020:1138 (CESA-2020:1138)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012451.html>

BDU:2021-01384 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01384>

RHSA-2020:2846 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2846>

RHSA-2020:2485 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2485>

RHSA-2020:1138 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1138>

CVE-2018-18751 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 4.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

CWE-415

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18751>

RHSA-2019:3643 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3643>

Уязвимость

Риск: Низкий

ALTX ID
307178

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-10638)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-10638.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:120763

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:120763>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

RHSA-2020:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1070>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

RHSA-2019:3517 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3517>

BDU:2019-02915 (FSTEC)

<https://bdu.fstec.ru/vul/2019-02915>

CVE-2019-10638 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
 CVSSv3: Базовая оценка 3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
 CWE-326
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10638>

RHSA-2019:3309 (VENDOR)

<https://access.redhat.com/errata/RHSA-2019:3309>

Уязвимость	Риск: Низкий
ALTX ID 317784	Red Hat/CentOS -- уязвимость в Bind (CVE-2019-6465)
Описание	

В продукте Bind обнаружена уязвимость CVE-2019-6465.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:127670
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:127670>

CESA-2020:1061 (CESA-2020:1061)
<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012415.html>

RHSA-2020:1061 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:1061>

BDU:2020-00612 (FSTEC)
<https://bdu.fstec.ru/vul/2020-00612>

CVE-2019-6465 (CVE)
 CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
 CVSSv3: Базовая оценка 3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
 CWE-732
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6465>

RHSA-2019:3552 (VENDOR)
<https://access.redhat.com/errata/RHSA-2019:3552>

Уязвимость	Риск: Низкий
ALTX ID 318588	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2019-17055)
Описание	

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2019-17055.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:128166
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:128166>

CESA-2020:0790 (CESA-2020:0790)
<http://lists.centos.org/pipermail/centos-announce/2020-March/035659.html>

CESA-2020:4060 (CESA-2020:4060)
<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:4060>**RHSA-2020:4062 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:4062>**RHSA-2020:1567 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1567>**RHSA-2020:1769 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1769>**BDU:2020-01324 (FSTEC)**<https://bdu.fstec.ru/vul/2020-01324>**CVE-2019-17055 (CVE)**

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 4.0 (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

CWE-862

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17055>**RHSA-2020:0790 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:0790>

Уязвимость	Риск: Низкий
ALTX ID 320057	Red Hat/CentOS -- уязвимость в libxml2 (CVE-2015-8035)
Описание	

В продукте libxml2 обнаружена уязвимость CVE-2015-8035.

Исправление	
-------------	--

Необходимо установить актуальное обновление от производителя.

Ссылки	
--------	--

oval:ru.altx-soft.nix:def:129105<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129105>**BDU:2015-12119 (FSTEC)**<https://bdu.fstec.ru/vul/2015-12119>**CESA-2020:1190 (CESA-2020:1190)**<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012518.html>**CVE-2015-8035 (CVE)**

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CWE-399

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8035>**RHSA-2020:1190 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:1190>

Уязвимость	Риск: Низкий
ALTX ID 320058	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2015-9289)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2015-9289.

Исправление	
-------------	--

Необходимо установить актуальное обновление от производителя.

Ссылки	
--------	--

oval:ru.altx-soft.nix:def:129106

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129106>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

CVE-2015-9289 (CVE)

CVSSv2: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:C/I:N/A:N)

CVSSv3: Базовая оценка 3.2 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

CWE-125

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9289>

RHSA-2020:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1070>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

Уязвимость

Риск: Низкий

ALTX ID

320065

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2017-17807)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2017-17807.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129113

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129113>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

CVE-2017-17807 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 3.2 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)

CWE-862

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17807>

RHSA-2020:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1070>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

Уязвимость

Риск: Низкий

ALTX ID

320069

Red Hat/CentOS -- уязвимость в libxml2 (CVE-2017-18258)

Описание

В продукте libxml2 обнаружена уязвимость CVE-2017-18258.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129117

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129117>

BDU:2021-03356 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03356>

CESA-2020:1190 (CESA-2020:1190)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012518.html>

CVE-2017-18258 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 3.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L)

CWE-770

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18258>

RHSA-2020:1190 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1190>

Уязвимость	Риск: Низкий
ALTX ID 320084	Red Hat/CentOS -- уязвимость в polkit (CVE-2018-1116)
Описание	

В продукте polkit обнаружена уязвимость CVE-2018-1116.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129132

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129132>

CESA-2020:1135 (CESA-2020:1135)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012566.html>

CVE-2018-1116 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:P/I:N/A:P)

CVSSv3: Базовая оценка 4.4 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L)

CWE-862

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1116>

RHSA-2020:1135 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1135>

Уязвимость	Риск: Низкий
ALTX ID 320090	Red Hat/CentOS -- уязвимость в httpd (CVE-2018-1301)
Описание	

В продукте httpd обнаружена уязвимость CVE-2018-1301.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129138

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129138>

CESA-2020:1121 (CESA-2020:1121)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012463.html>

BDU:2019-04309 (FSTEC)

<https://bdu.fstec.ru/vul/2019-04309>

CVE-2018-1301 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
 CVSSv3: Базовая оценка 3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)
 CWE-119
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1301>

RHSA-2020:1121 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1121>

Уязвимость	Риск: Низкий
ALTX ID 320132	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-10639)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-10639.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

- oval:ru.altx-soft.nix:def:129180**
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129180>
- CESA-2020:1016 (CESA-2020:1016)**
<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>
- RHSA-2020:2522 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:2522>
- RHSA-2020:1567 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:1567>
- RHSA-2020:1769 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:1769>
- BDU:2019-02762 (FSTEC)**
<https://bdu.fstec.ru/vul/2019-02762>
- CVE-2019-10639 (CVE)**
CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSSv3: Базовая оценка 3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
CWE-326
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10639>
- RHSA-2020:1070 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:1070>
- RHSA-2020:1016 (VENDOR)**
<https://access.redhat.com/errata/RHSA-2020:1016>

Уязвимость	Риск: Низкий
ALTX ID 320134	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-11190)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-11190.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:129182

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:129182>

BDU:2022-03979 (FSTEC)

<https://bdu.fstec.ru/vul/2022-03979>

CESA-2020:1016 (CESA-2020:1016)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-April/012401.html>

CVE-2019-11190 (CVE)

CVSSv2: Базовая оценка 4.6 (AV:L/AC:M/Au:N/C:C/I:N/A:N)

CVSSv3: Базовая оценка 3.2 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

CWE-362

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11190>

RHSA-2020:1070 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1070>

RHSA-2020:1016 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1016>

Уязвимость

Риск: Низкий

ALTX ID

323684

Red Hat/CentOS -- уязвимость в libtiff (CVE-2019-14973)

Описание

В продукте libtiff обнаружена уязвимость CVE-2019-14973.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:130804

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:130804>

CESA-2020:3902 (CESA-2020:3902)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012763.html>

RHSA-2020:3902 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3902>

BDU:2020-00107 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00107>

CVE-2019-14973 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 4.5 (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L)

CWE-190

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14973>

RHSA-2020:1688 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1688>

Уязвимость

Риск: Низкий

ALTX ID

323687

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-17053)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-17053.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:130807

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:130807>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

BDU:2020-01322 (FSTEC)

<https://bdu.fstec.ru/vul/2020-01322>

CVE-2019-17053 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 4.0 (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L)

CWE-276

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17053>

RHSA-2020:1567 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1567>

RHSA-2020:1769 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1769>

Уязвимость

Риск: Низкий

ALT X ID

324127

Red Hat/CentOS -- уязвимость в libmspack (CVE-2019-1010305)

Описание

В продукте libmspack обнаружена уязвимость CVE-2019-1010305.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:131162

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:131162>

CESA-2020:3848 (CESA-2020:3848)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012755.html>

RHSA-2020:3848 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3848>

BDU:2020-01531 (FSTEC)

<https://bdu.fstec.ru/vul/2020-01531>

CVE-2019-1010305 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 2.5 (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N)

CWE-119

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1010305>

RHSA-2020:1686 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1686>

Уязвимость

Риск: Низкий

ALT X ID

324147

Red Hat/CentOS -- уязвимость в dnsmasq (CVE-2019-14834)

Описание

В продукте dnsmasq обнаружена уязвимость CVE-2019-14834.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:131182

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:131182>

BDU:2022-06243 (FSTEC)

<https://bdu.fstec.ru/vul/2022-06243>

CESA-2020:3878 (CESA-2020:3878)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012682.html>

RHSA-2020:3878 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3878>

CVE-2019-14834 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)

CWE-770

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14834>

RHSA-2020:1715 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1715>

Уязвимость

Риск: Низкий

ALTX ID

324161

Red Hat/CentOS -- уязвимость в glibc (CVE-2019-19126)

Описание

В продукте glibc обнаружена уязвимость CVE-2019-19126.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:131196

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:131196>

BDU:2022-05763 (FSTEC)

<https://bdu.fstec.ru/vul/2022-05763>

CESA-2020:3861 (CESA-2020:3861)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012713.html>

RHSA-2020:3861 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3861>

CVE-2019-19126 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 2.9 (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CWE-665

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19126>

RHSA-2020:1828 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1828>

Уязвимость

Риск: Низкий

ALTX ID

324173

Red Hat/CentOS -- уязвимость в cups (CVE-2019-8675)

Описание

В продукте cups обнаружена уязвимость CVE-2019-8675.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:131208

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:131208>

CESA-2020:3864 (CESA-2020:3864)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012674.html>

RHSA-2020:3864 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3864>

BDU:2020-02389 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02389>

CVE-2019-8675 (CVE)

CVSSv2: Базовая оценка 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

CVSSv3: Базовая оценка 3.5 (CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L)

CWE-120

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8675>

RHSA-2020:1765 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1765>

Уязвимость

Риск: Низкий

ALTX ID

324174

Red Hat/CentOS -- уязвимость в cups (CVE-2019-8696)

Описание

В продукте cups обнаружена уязвимость CVE-2019-8696.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:131209

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:131209>

CESA-2020:3864 (CESA-2020:3864)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012674.html>

RHSA-2020:3864 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3864>

BDU:2020-02388 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02388>

CVE-2019-8696 (CVE)

CVSSv2: Базовая оценка 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

CVSSv3: Базовая оценка 3.5 (CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L)

CWE-120

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8696>

RHSA-2020:1765 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:1765>

Уязвимость

Риск: Низкий

ALTX ID
326424

Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-0548)

Описание

В продукте microcode_ctl обнаружена уязвимость CVE-2020-0548.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:132632

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:132632>

RHSA-2021:3364 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3364>

RHSA-2021:3322 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3322>

RHSA-2021:3317 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3317>

RHSA-2021:3323 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3323>

RHSA-2021:3176 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3176>

RHSA-2021:3255 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3255>

RHSA-2021:3028 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3028>

CESA-2021:3028 (CESA-2021:3028)

<http://lists.centos.org/pipermail/centos-announce/2021-August/048347.html>

RHSA-2021:3029 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3029>

RHSA-2021:3027 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3027>

CESA-2020:2433 (CESA-2020:2433)

<http://lists.centos.org/pipermail/centos-announce/2020-June/035752.html>

RHSA-2020:2842 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2842>

RHSA-2020:2432 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2432>

CESA-2020:2432 (CESA-2020:2432)

<http://lists.centos.org/pipermail/centos-announce/2020-June/035754.html>

RHSA-2020:2758 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2758>

RHSA-2020:2771 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2771>

RHSA-2020:2677 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2677>

RHSA-2020:2679 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2679>

RHSA-2020:2680 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:2680>

RHSA-2020:2706 (VENDOR)<https://access.redhat.com/errata/RHSA-2020:2706>**RHSA-2020:2707 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:2707>**BDU:2020-00306 (FSTEC)**<https://bdu.fstec.ru/vul/2020-00306>**CVE-2020-0548 (CVE)**

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 2.7 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:N)

CWE-404

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0548>**RHSA-2020:2433 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:2433>**RHSA-2020:2431 (VENDOR)**<https://access.redhat.com/errata/RHSA-2020:2431>

Уязвимость	Риск: Низкий
ALTX ID 333906	Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2020-12402)
Описание	

В продуктах nspr, nss обнаружена уязвимость CVE-2020-12402.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:138456

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:138456>

CESA-2020:4076-CentOS 7 (CESA-2020:4076)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-November/012876.html>

RHSA-2020:4076 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4076>

BDU:2020-04504 (FSTEC)

<https://bdu.fstec.ru/vul/2020-04504>

CVE-2020-12402 (CVE)

CVSSv2: Базовая оценка 1.2 (AV:L/AC:H/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 4.4 (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N)

CWE-203

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12402>

RHSA-2020:3280 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3280>

Уязвимость	Риск: Низкий
ALTX ID 337341	Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-16231)
Описание	

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-16231.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140473

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140473>

BDU:2022-07033 (FSTEC)

<https://bdu.fstec.ru/vul/2022-07033>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2019-16231 (CVE)

CVSSv2: Базовая оценка 4.6 (AV:L/AC:M/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 4.0 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16231>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Низкий

ALT X ID

337342

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-16233)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-16233.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140474

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140474>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2019-16233 (CVE)

CVSSv2: Базовая оценка 4.6 (AV:L/AC:M/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 4.0 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16233>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Низкий

ALTX ID

337356

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2019-19537)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2019-19537.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140488

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140488>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

BDU:2020-00289 (FSTEC)

<https://bdu.fstec.ru/vul/2020-00289>

CVE-2019-19537 (CVE)

CVSSv2: Базовая оценка 4.6 (AV:L/AC:M/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 4.1 (CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

CWE-362

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19537>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость

Риск: Низкий

ALTX ID

337364

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-10732)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-10732.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140496

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140496>

BDU:2021-03057 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03057>

RHSA-2020:4609 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4609>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

CVE-2020-10732 (CVE)

CVSSv2: Базовая оценка 3.5 (AV:L/AC:L/Au:N/C:P/I:N/A:P)
 CVSSv3: Базовая оценка 3.2 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)
 CWE-908
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10732>

RHSA-2020:4062 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4062>

Уязвимость	Риск: Низкий
ALTX ID 337756	Red Hat/CentOS -- уязвимость в httpd (CVE-2017-15715)
Описание	

В продукте httpd обнаружена уязвимость CVE-2017-15715.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140823
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140823>

BDU:2019-04106 (FSTEC)
<https://bdu.fstec.ru/vul/2019-04106>

CESA-2020:3958 (CESA-2020:3958)
<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012727.html>

CVE-2017-15715 (CVE)
 CVSSv2: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
 CVSSv3: Базовая оценка 3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)
 CWE-20
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15715>

RHSA-2020:3958 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3958>

Уязвимость	Риск: Низкий
ALTX ID 337769	Red Hat/CentOS -- уязвимость в httpd:2.4 (CVE-2019-10098)
Описание	

В продукте httpd:2.4 обнаружена уязвимость CVE-2019-10098.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140836
<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140836>

BDU:2019-03652 (FSTEC)
<https://bdu.fstec.ru/vul/2019-03652>

RHSA-2020:4751 (VENDOR)
<https://access.redhat.com/errata/RHSA-2020:4751>

CESA-2020:3958 (CESA-2020:3958)
<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012727.html>

BDU:2020-01010 (FSTEC)

<https://bdu.fstec.ru/vul/2020-01010>

CVE-2019-10098 (CVE)

CVSSv2: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)

CVSSv3: Базовая оценка 3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)

CWE-601

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10098>

RHSA-2020:3958 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3958>

Уязвимость	Риск: Низкий
ALT X ID 337774	Red Hat/CentOS -- уязвимость в kernel (CVE-2019-12614)
Описание	

В продукте kernel обнаружена уязвимость CVE-2019-12614.

Исправление	
--------------------	--

Необходимо установить актуальное обновление от производителя.

Ссылки	
---------------	--

oval:ru.altx-soft.nix:def:140841

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140841>

RHSA-2020:4431 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4431>

CESA-2020:4060 (CESA-2020:4060)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012745.html>

BDU:2020-02919 (FSTEC)

<https://bdu.fstec.ru/vul/2020-02919>

CVE-2019-12614 (CVE)

CVSSv2: Базовая оценка 4.6 (AV:L/AC:M/Au:N/C:N/I:N/A:C)

CVSSv3: Базовая оценка 4.0 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H)

CWE-476

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12614>

RHSA-2020:4060 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4060>

Уязвимость	Риск: Низкий
ALT X ID 337788	Red Hat/CentOS -- уязвимость в systemd (CVE-2019-20386)
Описание	

В продукте systemd обнаружена уязвимость CVE-2019-20386.

Исправление	
--------------------	--

Необходимо установить актуальное обновление от производителя.

Ссылки	
---------------	--

oval:ru.altx-soft.nix:def:140855

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140855>

BDU:2020-05729 (FSTEC)

<https://bdu.fstec.ru/vul/2020-05729>

RHSA-2020:4553 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4553>

CESA-2020:4007 (CESA-2020:4007)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012847.html>

CVE-2019-20386 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVSSv3: Базовая оценка 2.4 (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

CWE-401

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20386>

RHSA-2020:4007 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4007>

Уязвимость

Риск: Низкий

ALTX ID

337903

Red Hat/CentOS -- уязвимость в NetworkManager (CVE-2020-10754)

Описание

В продукте NetworkManager обнаружена уязвимость CVE-2020-10754.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140970

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140970>

CESA-2020:4003 (CESA-2020:4003)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012785.html>

CVE-2020-10754 (CVE)

CVSSv2: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:P/I:N/A:N)

CVSSv3: Базовая оценка 4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

CWE-306

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10754>

RHSA-2020:3011 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3011>

RHSA-2020:4003 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4003>

Уязвимость

Риск: Низкий

ALTX ID

337912

Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2020-12400)

Описание

В продуктах nspr, nss обнаружена уязвимость CVE-2020-12400.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140979

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140979>

CESA-2020:4076-CentOS 7 (CESA-2020:4076)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-November/012876.html>

RHSA-2021:0538 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0538>

BDU:2020-03960 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03960>

CVE-2020-12400 (CVE)

CVSSv2: Базовая оценка 1.2 (AV:L/AC:H/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 4.4 (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N)

CWE-203

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12400>

RHSA-2020:4076 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4076>

Уязвимость

Риск: Низкий

ALTX ID

337913

Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2020-12401)

Описание

В продуктах nspr, nss обнаружена уязвимость CVE-2020-12401.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140980

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140980>

CESA-2020:4076-CentOS 7 (CESA-2020:4076)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-November/012876.html>

BDU:2020-03961 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03961>

CVE-2020-12401 (CVE)

CVSSv2: Базовая оценка 1.8 (AV:L/AC:M/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 4.4 (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N)

CWE-203

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12401>

RHSA-2020:4076 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4076>

Уязвимость

Риск: Низкий

ALTX ID

337932

Red Hat/CentOS -- уязвимость в httpd:2.4 (CVE-2020-1934)

Описание

В продукте httpd:2.4 обнаружена уязвимость CVE-2020-1934.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:140999

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:140999>

RHSA-2020:4751 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4751>

CESA-2020:3958 (CESA-2020:3958)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012727.html>

BDU:2020-03568 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03568>

CVE-2020-1934 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)

CWE-908

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1934>

RHSA-2020:3958 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3958>

Уязвимость	Риск: Низкий
ALTX ID 337978	Red Hat/CentOS -- уязвимость в nspr, nss (CVE-2020-6829)
Описание	

В продуктах nspr, nss обнаружена уязвимость CVE-2020-6829.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:141045

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:141045>

CESA-2020:4076-CentOS 7 (CESA-2020:4076)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-November/012876.html>

RHSA-2021:0538 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0538>

BDU:2020-03953 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03953>

CVE-2020-6829 (CVE)

CVSSv2: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 4.4 (CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:N)

NVD-CWE-noinfo

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6829>

RHSA-2020:4076 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4076>

Уязвимость	Риск: Низкий
ALTX ID 341337	Red Hat/CentOS -- уязвимость в kernel, kernel-rt (CVE-2019-20811)
Описание	

В продуктах kernel, kernel-rt обнаружена уязвимость CVE-2019-20811.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:143025

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:143025>

CESA-2020:5023 (CESA-2020:5023)

<http://lists.centos.org/pipermail/centos-announce/2020-November/035868.html>

BDU:2020-03025 (FSTEC)

<https://bdu.fstec.ru/vul/2020-03025>

CVE-2019-20811 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 3.2 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)

NVD-CWE-Other

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20811>

RHSA-2020:5023 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5023>

RHSA-2020:5026 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5026>

Уязвимость	Риск: Низкий
ALTX ID 341422	Red Hat/CentOS -- уязвимость в Bind (CVE-2020-8624)
Описание	

В продукте Bind обнаружена уязвимость CVE-2020-8624.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:143110

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:143110>

CESA-2020:5011 (CESA-2020:5011)

<http://lists.centos.org/pipermail/centos-announce/2020-November/035850.html>

BDU:2021-01726 (FSTEC)

<https://bdu.fstec.ru/vul/2021-01726>

RHSA-2020:5203 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5203>

CVE-2020-8624 (CVE)

CVSSv2: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:N/I:P/A:N)

CVSSv3: Базовая оценка 4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)

CWE-269

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8624>

RHSA-2020:4500 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:4500>

RHSA-2020:5011 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5011>

Уязвимость	Риск: Низкий
ALTX ID 341425	Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-8696)
Описание	

В продукте microcode_ctl обнаружена уязвимость CVE-2020-8696.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:143113

<https://ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:143113>

RHSA-2020:5186 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5186>

RHSA-2021:3364 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3364>

RHSA-2021:3322 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3322>

RHSA-2021:3317 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3317>

RHSA-2021:3323 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3323>

RHSA-2021:3176 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3176>

RHSA-2021:3255 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3255>

RHSA-2021:3028 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3028>

CESA-2021:3028 (CESA-2021:3028)

<http://lists.centos.org/pipermail/centos-announce/2021-August/048347.html>

RHSA-2021:3029 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3029>

RHSA-2021:3027 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3027>

CESA-2020:5083 (CESA-2020:5083)

<http://lists.centos.org/pipermail/centos-announce/2020-November/035872.html>

RHSA-2020:5369 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5369>

BDU:2020-05478 (FSTEC)

<https://bdu.fstec.ru/vul/2020-05478>

RHSA-2020:5181 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5181>

RHSA-2020:5182 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5182>

RHSA-2020:5183 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5183>

RHSA-2020:5184 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5184>

RHSA-2020:5185 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5185>

RHSA-2020:5188 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5188>

RHSA-2020:5189 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5189>

RHSA-2020:5190 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5190>

CVE-2020-8696 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 2.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:N)

CWE-212

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8696>

RHSA-2020:5083 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5083>

RHSA-2020:5084 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5084>

RHSA-2020:5085 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:5085>

Уязвимость	Риск: Низкий
ALT X ID 345785	Red Hat/CentOS -- уязвимость в dnsmasq (CVE-2020-25684)
Описание	

В продукте dnsmasq обнаружена уязвимость CVE-2020-25684.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:146337

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:146337>

BDU:2021-03624 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03624>

CESA-2021:0153 (CESA-2021:0153)

<http://lists.centos.org/pipermail/centos-announce/2021-January/048251.html>

RHSA-2021:0240 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0240>

RHSA-2021:0245 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0245>

CVE-2020-25684 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 4.0 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N)

NVD-CWE-Other

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25684>

RHSA-2021:0153 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0153>

RHSA-2021:0155 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0155>

RHSA-2021:0156 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0156>

RHSA-2021:0150 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0150>

RHSA-2021:0152 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0152>

RHSA-2021:0151 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0151>

RHSA-2021:0154 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0154>

Уязвимость	Риск: Низкий
ALT X ID 345786	Red Hat/CentOS -- уязвимость в dnsmasq (CVE-2020-25685)
Описание	

В продукте dnsmasq обнаружена уязвимость CVE-2020-25685.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:146338

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:146338>

BDU:2021-03623 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03623>

CESA-2021:0153 (CESA-2021:0153)

<http://lists.centos.org/pipermail/centos-announce/2021-January/048251.html>

RHSA-2021:0240 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0240>

RHSA-2021:0245 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0245>

CVE-2020-25685 (CVE)

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 4.0 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N)

CWE-326

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25685>

RHSA-2021:0153 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0153>

RHSA-2021:0155 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0155>

RHSA-2021:0156 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0156>

RHSA-2021:0150 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0150>

RHSA-2021:0152 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0152>

RHSA-2021:0151 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0151>

RHSA-2021:0154 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0154>

Уязвимость

Риск: Низкий

ALTX ID
345787

Red Hat/CentOS -- уязвимость в dnsmasq (CVE-2020-25686)

Описание

В продукте dnsmasq обнаружена уязвимость CVE-2020-25686.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:146339

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:146339>

BDU:2021-03619 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03619>

CESA-2021:0153 (CESA-2021:0153)

<http://lists.centos.org/pipermail/centos-announce/2021-January/048251.html>

RHSA-2021:0240 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:0240>

RHSA-2021:0245 (VENDOR)<https://access.redhat.com/errata/RHSA-2021:0245>**CVE-2020-25686 (CVE)**

CVSSv2: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

CVSSv3: Базовая оценка 4.0 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N)

CWE-358

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25686>**RHSA-2021:0153 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0153>**RHSA-2021:0155 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0155>**RHSA-2021:0156 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0156>**RHSA-2021:0150 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0150>**RHSA-2021:0152 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0152>**RHSA-2021:0151 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0151>**RHSA-2021:0154 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0154>

Уязвимость

Риск: Низкий

ALTX ID

350028

Red Hat/CentOS -- уязвимость в kernel-rt, kernel (CVE-2020-25656)

Описание

В продуктах kernel-rt, kernel обнаружена уязвимость CVE-2020-25656.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:148601

<https://ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:148601>

CESA-2021:0856 (CESA-2021:0856)

<http://lists.centos.org/pipermail/centos-announce/2021-March/048295.html>

BDU:2020-05831 (FSTEC)

<https://bdu.fstec.ru/vul/2020-05831>**CVE-2020-25656 (CVE)**

CVSSv2: Базовая оценка 1.8 (AV:L/AC:M/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 4.0 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N)

CWE-416

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25656>**RHSA-2021:0857 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0857>**RHSA-2021:0856 (VENDOR)**<https://access.redhat.com/errata/RHSA-2021:0856>

Уязвимость

Риск: Низкий

ALTX ID

357235

Red Hat/CentOS -- уязвимость в libpng (CVE-2017-12652)

Описание

В продукте libpng обнаружена уязвимость CVE-2017-12652.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:153597

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:153597>

CVE-2017-12652 (CVE)

CVSSv2: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSSv3: Базовая оценка 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CWE-20

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12652>

RHSA-2020:3901 (VENDOR)

<https://access.redhat.com/errata/RHSA-2020:3901>

CESA-2020:3901 (CESA-2020:3901)

<http://lists.centos.org/pipermail/centos-cr-announce/2020-October/012757.html>

Уязвимость

Риск: Низкий

ALTX ID

359158

Red Hat/CentOS -- уязвимость в microcode_ctl (CVE-2020-24512)

Описание

В продукте microcode_ctl обнаружена уязвимость CVE-2020-24512.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:155076

<https://ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:155076>

RHSA-2021:3364 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3364>

RHSA-2021:3322 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3322>

RHSA-2021:2304 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2304>

RHSA-2021:2305 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2305>

RHSA-2021:2308 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2308>

RHSA-2021:3317 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3317>

RHSA-2021:3323 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3323>

RHSA-2021:3176 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3176>

RHSA-2021:3255 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3255>

RHSA-2021:3028 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3028>

CESA-2021:3028 (CESA-2021:3028)

<http://lists.centos.org/pipermail/centos-announce/2021-August/048347.html>

RHSA-2021:3029 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3029>

RHSA-2021:3027 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:3027>

BDU:2021-03383 (FSTEC)

<https://bdu.fstec.ru/vul/2021-03383>

CVE-2020-24512 (CVE)

CVSSv2: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CVSSv3: Базовая оценка 3.2 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

CWE-203

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24512>

RHSA-2021:2300 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2300>

RHSA-2021:2299 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2299>

RHSA-2021:2301 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2301>

RHSA-2021:2302 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2302>

RHSA-2021:2306 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2306>

RHSA-2021:2303 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2303>

RHSA-2021:2307 (VENDOR)

<https://access.redhat.com/errata/RHSA-2021:2307>

Конец отчёта. RedCheckWeb 2.6.9.6467.
RedCheckID: 0F8F995B-1C1C-44ED-9832-EC3F21F9BF71.
© АО "АЛТЭК-СОФТ"