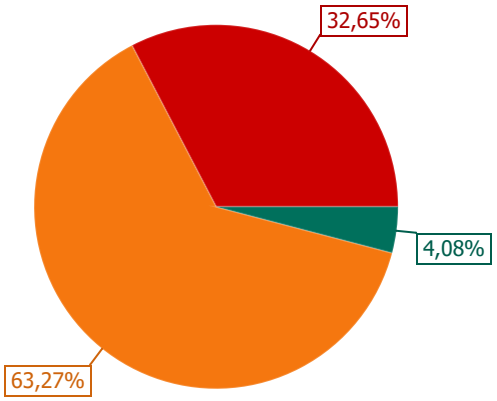
RED Check

ОТЧЁТ

№ отчёта	*28372e46-2ad9-46f8-a4e7-1fb649c4d83d*
Профиль	*Обновления*
Задание	*Job_8661*
Начало/завершение сканирования	*28.03.2018 17:41:09 / 28.03.2018 17:42:25*
Формирование отчёта	*28.03.2018 17:46:04*
Имя	*Quick_192.168.1.110_128*
Описание	*Автогенерируемый отчет вкладки "История" для "192.168.1.110" из "Job_8661" задания.*
Хосты [1]	*192.168.1.110*

Диаграмма распределения обновлений по уровням риска



Риск	*Количество*
Высокий	*16*
Средний	*31*
Низкий	*2*
Всего	*49*

Таблица распределения обновлений по хостам

Хост / Риск	Высокий	Средний	Низкий	Всего
192.168.1.110	*16*	*31*	*2*	*49*
Всего	**16**	**31**	**2**	**49**

Таблица распределения обновлений по продуктам

Продукт / Риск	Высокий	Средний	Низкий	Всего
cpe:/o:redhat:enterprise_linux:7	*16*	*31*	*2*	*49*
Всего	**16**	**31**	**2**	**49**

Хост: 192.168.1.110

CPE	*cpe:/o:redhat:enterprise_linux:7*
Начало/завершение сканирования	*28.03.2018 17:41:09 / 28.03.2018 17:42:25*
Учетные данные	*Имя профиля: Test* *Тип: Ssh* *Sudo: Да*
Метод получения данных	*Безагентный механизм*
Тип сканирования	*Полное*
Обновлений найдено	***49:*** ***16*** ***31*** ***2***

Обновления [49]

Хост	ALTX ID	Риск	Название
192.168.1.110	160951	Высокий	Обновление RHSA-2017:1106 : устранение уязвимостей в firefox (критичное)
cpe:/o:redhat:enterprise_linux:7			*firefox (0:52.0-6.el7)*
192.168.1.110	162852	Высокий	Обновление RHSA-2017:1440 : устранение уязвимостей в firefox (критичное)
cpe:/o:redhat:enterprise_linux:7			*firefox (0:52.0-6.el7)*
192.168.1.110	164624	Высокий	Обновление RHSA-2017:1789 : устранение уязвимостей в java-1.8.0-openjdk (критичное)
cpe:/o:redhat:enterprise_linux:7			*java-1.8.0-openjdk (1:1.8.0.131-7.b12.el7)*
			java-1.8.0-openjdk-headless (1:1.8.0.131-7.b12.el7)
192.168.1.110	172709	Высокий	Обновление RHSA-2018:0151 : устранение уязвимостей и ошибок в kernel (важное)
cpe:/o:redhat:enterprise_linux:7			*kernel (0:3.10.0-663.el7)*
			kernel-tools (0:3.10.0-663.el7)
			kernel-tools-libs (0:3.10.0-663.el7)
			python-perf (0:3.10.0-663.el7)
192.168.1.110	172710	Высокий	Обновление RHSA-2018:0122 : устранение уязвимостей в firefox (критичное)
cpe:/o:redhat:enterprise_linux:7			*firefox (0:52.0-6.el7)*
192.168.1.110	172767	Высокий	Обновление RHSA-2017:3368 : устранение уязвимостей в qemu-kvm (умеренное)
cpe:/o:redhat:enterprise_linux:7			*qemu-img (10:1.5.3-137.el7)*
			qemu-kvm (10:1.5.3-137.el7)
			qemu-kvm-common (10:1.5.3-137.el7)
192.168.1.110	172778	Высокий	Обновление RHSA-2017:3260 : устранение уязвимостей в samba (важное)
cpe:/o:redhat:enterprise_linux:7			*libsmbclient (0:4.6.2-1.el7)*
			libwbclient (0:4.6.2-1.el7)
			samba-client-libs (0:4.6.2-1.el7)
			samba-common (0:4.6.2-1.el7)
192.168.1.110	172779	Высокий	Обновление RHSA-2017:3247 : устранение уязвимостей в firefox (критичное)
cpe:/o:redhat:enterprise_linux:7			*firefox (0:52.0-6.el7)*
192.168.1.110	172792	Высокий	Обновление RHSA-2017:3075 : устранение уязвимостей в wget (важное)
cpe:/o:redhat:enterprise_linux:7			*wget (0:1.14-14.el7)*
192.168.1.110	172799	Высокий	Обновление RHSA-2017:2930 : устранение уязвимостей и ошибок в kernel (важное)
cpe:/o:redhat:enterprise_linux:7			*kernel (0:3.10.0-663.el7)*
			kernel-tools (0:3.10.0-663.el7)
			kernel-tools-libs (0:3.10.0-663.el7)
			python-perf (0:3.10.0-663.el7)

192.168.1.110	172813	Высокий	Обновление RHSA-2017:2836 : устранение уязвимостей в dnsmasq (критичное)
cpe:/o:redhat:enterprise_linux:7			*dnsmasq (0:2.76-2.el7)*
192.168.1.110	172815	Высокий	Обновление RHSA-2017:2831 : устранение уязвимостей в firefox (критичное)
cpe:/o:redhat:enterprise_linux:7			*firefox (0:52.0-6.el7)*
192.168.1.110	172830	Высокий	Обновление RHSA-2017:2788 : устранение уязвимостей в augeas (важное)
cpe:/o:redhat:enterprise_linux:7			*augeas-libs (0:1.4.0-2.el7)*
192.168.1.110	172845	Высокий	Обновление RHSA-2017:2679 : устранение уязвимостей в kernel (важное)
cpe:/o:redhat:enterprise_linux:7			*kernel (0:3.10.0-663.el7)*
			kernel-tools (0:3.10.0-663.el7)
			kernel-tools-libs (0:3.10.0-663.el7)
			python-perf (0:3.10.0-663.el7)
192.168.1.110	172929	Высокий	Обновление RHSA-2018:0527 : устранение уязвимостей в firefox (критичное)
cpe:/o:redhat:enterprise_linux:7			*firefox (0:52.0-6.el7)*
192.168.1.110	173269	Высокий	Обновление RHSA-2018:0549 : устранение уязвимостей в firefox (критичное)
cpe:/o:redhat:enterprise_linux:7			*firefox (0:52.0-6.el7)*
192.168.1.110	161434	Средний	Обновление RHSA-2017:1208 : устранение уязвимостей в jasper (важное)
cpe:/o:redhat:enterprise_linux:7			*jasper-libs (0:1.900.1-29.el7)*
192.168.1.110	163880	Средний	Обновление RHSA-2017:1680 : устранение уязвимостей и ошибок в bind (важное)
cpe:/o:redhat:enterprise_linux:7			*bind-libs (32:9.9.4-49.el7)*
			bind-libs-lite (32:9.9.4-49.el7)
			bind-license (32:9.9.4-49.el7)
			bind-utils (32:9.9.4-49.el7)
192.168.1.110	164628	Средний	Обновление RHSA-2017:1793 : устранение уязвимостей в graphite2 (важное)
cpe:/o:redhat:enterprise_linux:7			*graphite2 (0:1.3.6-1.el7_2)*
192.168.1.110	172679	Средний	Обновление RHSA-2018:0483 : устранение уязвимостей в dhcp (важное)
cpe:/o:redhat:enterprise_linux:7			*dhclient (12:4.2.5-53.el7)*
			dhcp-common (12:4.2.5-53.el7)
			dhcp-libs (12:4.2.5-53.el7)
192.168.1.110	172683	Средний	Обновление RHSA-2018:0418 : устранение уязвимостей в libreoffice (умеренное)
cpe:/o:redhat:enterprise_linux:7			*libreoffice-core (1:5.0.6.2-9.el7)*
			libreoffice-opensymbol-fonts (1:5.0.6.2-9.el7)
			libreoffice-ure (1:5.0.6.2-9.el7)
			libreofficekit (1:5.0.6.2-9.el7)
192.168.1.110	172685	Средний	Обновление RHSA-2018:0395 : устранение уязвимостей и ошибок в kernel (важное)
cpe:/o:redhat:enterprise_linux:7			*kernel (0:3.10.0-663.el7)*
			kernel-tools (0:3.10.0-663.el7)
			kernel-tools-libs (0:3.10.0-663.el7)
			python-perf (0:3.10.0-663.el7)
192.168.1.110	172694	Средний	Обновление RHSA-2018:0350 : устранение уязвимостей в gcab (важное)
cpe:/o:redhat:enterprise_linux:7			*libgcab1 (0:0.7-3.el7)*
192.168.1.110	172701	Средний	Обновление RHSA-2018:0260 : устранение уязвимостей в systemd (умеренное)
cpe:/o:redhat:enterprise_linux:7			*libgudev1 (0:219-39.el7)*
			systemd (0:219-39.el7)
			systemd-libs (0:219-39.el7)
			systemd-python (0:219-39.el7)
			systemd-sysv (0:219-39.el7)
192.168.1.110	172703	Средний	Обновление RHSA-2018:0223 : устранение уязвимостей в nautilus (умеренное)
cpe:/o:redhat:enterprise_linux:7			*nautilus (0:3.22.3-1.el7)*

			nautilus-extensions (0:3.22.3-1.el7)
192.168.1.110	172707	Средний	Обновление RHSA-2018:0158 : устранение уязвимостей в dhcp (умеренное)
cpe:/o:redhat:enterprise_linux:7			*dhclient (12:4.2.5-53.el7)*
			dhcp-common (12:4.2.5-53.el7)
			dhcp-libs (12:4.2.5-53.el7)
192.168.1.110	172721	Средний	Обновление RHSA-2018:0102 : устранение уязвимостей в bind (важное)
cpe:/o:redhat:enterprise_linux:7			*bind-libs (32:9.9.4-49.el7)*
			bind-libs-lite (32:9.9.4-49.el7)
			bind-license (32:9.9.4-49.el7)
			bind-utils (32:9.9.4-49.el7)
192.168.1.110	172723	Средний	Обновление RHSA-2018:0095 : устранение уязвимостей в java-1.8.0-openjdk (важное)
cpe:/o:redhat:enterprise_linux:7			*java-1.8.0-openjdk (1:1.8.0.131-7.b12.el7)*
			java-1.8.0-openjdk-headless (1:1.8.0.131-7.b12.el7)
192.168.1.110	172724	Средний	Обновление RHSA-2018:0094 : устранение уязвимостей в linux-firmware (важное)
cpe:/o:redhat:enterprise_linux:7			*iwl100-firmware (0:39.31.5.1-52.el7)*
			iwl1000-firmware (1:39.31.5.1-52.el7)
			iwl105-firmware (0:18.168.6.1-52.el7)
			iwl135-firmware (0:18.168.6.1-52.el7)
			iwl2000-firmware (0:18.168.6.1-52.el7)
			iwl2030-firmware (0:18.168.6.1-52.el7)
			iwl3160-firmware (0:22.0.7.0-52.el7)
			iwl3945-firmware (0:15.32.2.9-52.el7)
			iwl4965-firmware (0:228.61.2.24-52.el7)
			iwl5000-firmware (0:8.83.5.1_1-52.el7)
			iwl5150-firmware (0:8.24.2.2-52.el7)
			iwl6000-firmware (0:9.221.4.1-52.el7)
			iwl6000g2a-firmware (0:17.168.5.3-52.el7)
			iwl6000g2b-firmware (0:17.168.5.2-52.el7)
			iwl6050-firmware (0:41.28.5.1-52.el7)
			iwl7260-firmware (0:22.0.7.0-52.el7)
			iwl7265-firmware (0:22.0.7.0-52.el7)
			linux-firmware (0:20170328-52.git44d8e8d.el7)
192.168.1.110	172725	Средний	Обновление RHSA-2018:0093 : устранение уязвимостей в microcode_ctl (важное)
cpe:/o:redhat:enterprise_linux:7			*microcode_ctl (2:2.1-21.el7)*
192.168.1.110	172730	Средний	Обновление RHSA-2018:0029 : устранение уязвимостей в libvirt (важное)
cpe:/o:redhat:enterprise_linux:7			*libvirt-daemon (0:3.2.0-4.el7)*
			libvirt-daemon-config-network (0:3.2.0-4.el7)
			libvirt-daemon-driver-interface (0:3.2.0-4.el7)
			libvirt-daemon-driver-network (0:3.2.0-4.el7)
			libvirt-daemon-driver-nodedev (0:3.2.0-4.el7)
			libvirt-daemon-driver-nwfilter (0:3.2.0-4.el7)
			libvirt-daemon-driver-qemu (0:3.2.0-4.el7)
			libvirt-daemon-driver-secret (0:3.2.0-4.el7)
			libvirt-daemon-driver-storage (0:3.2.0-4.el7)
			libvirt-daemon-driver-storage-core (0:3.2.0-4.el7)
			libvirt-daemon-driver-storage-disk (0:3.2.0-4.el7)
			libvirt-daemon-driver-storage-gluster (0:3.2.0-4.el7)
			libvirt-daemon-driver-storage-iscsi (0:3.2.0-4.el7)
			libvirt-daemon-driver-storage-logical (0:3.2.0-4.el7)
			libvirt-daemon-driver-storage-mpath (0:3.2.0-4.el7)

			libvirt-daemon-driver-storage-rbd (0:3.2.0-4.el7)
			libvirt-daemon-driver-storage-scsi (0:3.2.0-4.el7)
			libvirt-daemon-kvm (0:3.2.0-4.el7)
			libvirt-libs (0:3.2.0-4.el7)
192.168.1.110	172743	Средний	Обновление RHSA-2018:0023 : устранение уязвимостей в qemu-kvm (важное)
cpe:/o:redhat:enterprise_linux:7			*qemu-img (10:1.5.3-137.el7)*
			qemu-kvm (10:1.5.3-137.el7)
			qemu-kvm-common (10:1.5.3-137.el7)
192.168.1.110	172750	Средний	Обновление RHSA-2018:0014 : устранение уязвимостей в linux-firmware (важное)
cpe:/o:redhat:enterprise_linux:7			*iwl100-firmware (0:39.31.5.1-52.el7)*
			iwl1000-firmware (1:39.31.5.1-52.el7)
			iwl105-firmware (0:18.168.6.1-52.el7)
			iwl135-firmware (0:18.168.6.1-52.el7)
			iwl2000-firmware (0:18.168.6.1-52.el7)
			iwl2030-firmware (0:18.168.6.1-52.el7)
			iwl3160-firmware (0:22.0.7.0-52.el7)
			iwl3945-firmware (0:15.32.2.9-52.el7)
			iwl4965-firmware (0:228.61.2.24-52.el7)
			iwl5000-firmware (0:8.83.5.1_1-52.el7)
			iwl5150-firmware (0:8.24.2.2-52.el7)
			iwl6000-firmware (0:9.221.4.1-52.el7)
			iwl6000g2a-firmware (0:17.168.5.3-52.el7)
			iwl6000g2b-firmware (0:17.168.5.2-52.el7)
			iwl6050-firmware (0:41.28.5.1-52.el7)
			iwl7260-firmware (0:22.0.7.0-52.el7)
			iwl7265-firmware (0:22.0.7.0-52.el7)
			linux-firmware (0:20170328-52.git44d8e8d.el7)
192.168.1.110	172752	Средний	Обновление RHSA-2018:0012 : устранение уязвимостей в microcode_ctl (важное)
cpe:/o:redhat:enterprise_linux:7			*microcode_ctl (2:2.1-21.el7)*
192.168.1.110	172757	Средний	Обновление RHSA-2018:0007 : устранение уязвимостей в kernel (важное)
cpe:/o:redhat:enterprise_linux:7			*kernel (0:3.10.0-663.el7)*
			kernel-tools (0:3.10.0-663.el7)
			kernel-tools-libs (0:3.10.0-663.el7)
			python-perf (0:3.10.0-663.el7)
192.168.1.110	172762	Средний	Обновление RHSA-2017:3384 : устранение уязвимостей в liblouis (умеренное)
cpe:/o:redhat:enterprise_linux:7			*liblouis (0:2.5.2-10.el7)*
			liblouis-python (0:2.5.2-10.el7)
192.168.1.110	172763	Средний	Обновление RHSA-2017:3382 : устранение уязвимостей в firefox (важное)
cpe:/o:redhat:enterprise_linux:7			*firefox (0:52.0-6.el7)*
192.168.1.110	172764	Средний	Обновление RHSA-2017:3379 : устранение уязвимостей и ошибок в sssd (умеренное)
cpe:/o:redhat:enterprise_linux:7			*libsss_idmap (0:1.15.2-24.el7)*
			libsss_nss_idmap (0:1.15.2-24.el7)
			sssd-client (0:1.15.2-24.el7)
192.168.1.110	172777	Средний	Обновление RHSA-2017:3263 : устранение уязвимостей в curl (умеренное)
cpe:/o:redhat:enterprise_linux:7			*curl (0:7.29.0-42.el7)*
			libcurl (0:7.29.0-42.el7)
192.168.1.110	172787	Средний	Обновление RHSA-2017:3111 : устранение уязвимостей в liblouis (умеренное)
cpe:/o:redhat:enterprise_linux:7			*liblouis (0:2.5.2-10.el7)*
			liblouis-python (0:2.5.2-10.el7)

192.168.1.110	172794	Средний	Обновление RHSA-2017:2998 : устранение уязвимостей в java-1.8.0-openjdk (критичное)
cpe:/o:redhat:enterprise_linux:7			*java-1.8.0-openjdk (1:1.8.0.131-7.b12.el7)*
			java-1.8.0-openjdk-headless (1:1.8.0.131-7.b12.el7)
192.168.1.110	172801	Средний	Обновление RHSA-2017:2907 : устранение уязвимостей в wpa_supplicant (важное)
cpe:/o:redhat:enterprise_linux:7			*wpa_supplicant (1:2.6-4.el7)*
192.168.1.110	172814	Средний	Обновление RHSA-2017:2832 : устранение уязвимостей в nss (важное)
cpe:/o:redhat:enterprise_linux:7			*nss (0:3.28.4-6.el7)*
			nss-sysinit (0:3.28.4-6.el7)
			nss-tools (0:3.28.4-6.el7)
192.168.1.110	172828	Средний	Обновление RHSA-2017:2790 : устранение уязвимостей в samba (умеренное)
cpe:/o:redhat:enterprise_linux:7			*libsmbclient (0:4.6.2-1.el7)*
			libwbclient (0:4.6.2-1.el7)
			samba-client-libs (0:4.6.2-1.el7)
			samba-common (0:4.6.2-1.el7)
192.168.1.110	172831	Средний	Обновление RHSA-2017:2771 : устранение уязвимостей в emacs (важное)
cpe:/o:redhat:enterprise_linux:7			*emacs-filesystem (1:24.3-19.el7_3)*
192.168.1.110	172852	Средний	Обновление RHSA-2017:2551 : устранение уязвимостей в poppler (умеренное)
cpe:/o:redhat:enterprise_linux:7			*poppler (0:0.26.5-16.el7)*
			poppler-glib (0:0.26.5-16.el7)
			poppler-utils (0:0.26.5-16.el7)
192.168.1.110	172856	Средний	Обновление RHSA-2017:2492 : устранение уязвимостей в xmlsec1 (умеренное)
cpe:/o:redhat:enterprise_linux:7			*xmlsec1 (0:1.2.20-5.el7)*
			xmlsec1-openssl (0:1.2.20-5.el7)
192.168.1.110	172770	Низкий	Обновление RHSA-2017:3315 : устранение уязвимостей и ошибок в kernel (умеренное)
cpe:/o:redhat:enterprise_linux:7			*kernel (0:3.10.0-663.el7)*
			kernel-tools (0:3.10.0-663.el7)
			kernel-tools-libs (0:3.10.0-663.el7)
			python-perf (0:3.10.0-663.el7)
192.168.1.110	172841	Низкий	Обновление RHSA-2017:2685 : устранение уязвимостей в bluez (умеренное)
cpe:/o:redhat:enterprise_linux:7			*bluez (0:5.44-2.el7)*

Список обновлений

Обновление Риск: Высокий

ALTX ID	Обновление RHSA-2017:1106 : устранение уязвимостей в firefox (критичное)
160951	

Описание

Multiple flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:25370
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:25370

RHSA-2017:1106 (VENDOR)
https://rhn.redhat.com/errata/RHSA-2017-1106.html

CESA-2017:1106 (CESA-2017:1106)
http://lists.centos.org/pipermail/centos-announce/2017-April/022398.html

CVE-2017-5429 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5429

CVE-2017-5430 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5430

CVE-2017-5432 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5432

CVE-2017-5433 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5433

CVE-2017-5434 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5434

CVE-2017-5435 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5435

CVE-2017-5436 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5436

CVE-2017-5437 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5437

CVE-2017-5438 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5438

CVE-2017-5439 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5439

CVE-2017-5440 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5440

CVE-2017-5441 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5441

CVE-2017-5442 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5442

CVE-2017-5443 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5443

CVE-2017-5444 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5444

CVE-2017-5445 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5445

CVE-2017-5446 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5446

CVE-2017-5447 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5447

CVE-2017-5448 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5448

CVE-2017-5449 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5449

CVE-2017-5451 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5451

CVE-2017-5454 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5454

CVE-2017-5455 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5455

CVE-2017-5456 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5456

CVE-2017-5459 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5459

CVE-2017-5460 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5460

CVE-2017-5464 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5464

CVE-2017-5465 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5465

CVE-2017-5466 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5466

CVE-2017-5467 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5467

CVE-2017-5469 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5469

Обновление Риск: Высокий

ALTX ID 162852

Обновление RHSA-2017:1440 : устранение уязвимостей в firefox (критичное)

Описание

Multiple flaws were found in the processing of malformed web content. A web page containing malicious content could cause Firefox to crash or, potentially, execute arbitrary code with the privileges of the user running Firefox.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:27622
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:27622

RHSA-2017:1440 (VENDOR)
https://rhn.redhat.com/errata/RHSA-2017-1440.html

CESA-2017:1440-CentOS 6 (CESA-2017:1440)
http://lists.centos.org/pipermail/centos-announce/2017-June/022459.html

CESA-2017:1440-CentOS 7 (CESA-2017:1440)
http://lists.centos.org/pipermail/centos-announce/2017-June/022460.html

CVE-2017-5470 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5470

CVE-2017-5472 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5472

CVE-2017-7749 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7749

CVE-2017-7750 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7750

CVE-2017-7751 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7751

CVE-2017-7752 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7752

CVE-2017-7754 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7754

CVE-2017-7756 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7756

CVE-2017-7757 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7757

CVE-2017-7758 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7758

CVE-2017-7764 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7764

CVE-2017-7771 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7771

CVE-2017-7772 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7772

CVE-2017-7773 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7773

CVE-2017-7774 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7774

CVE-2017-7775 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7775

CVE-2017-7776 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7776

CVE-2017-7777 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7777

CVE-2017-7778 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7778

Обновление Риск: Высокий

ALTX ID 164624	**Обновление RHSA-2017:1789 : устранение уязвимостей в java-1.8.0-openjdk (критичное)**

Описание

Multiple vulnerabilities in java.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:28334
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:28334

RHSA-2017:1789 (VENDOR)
https://rhn.redhat.com/errata/RHSA-2017-1789.html

CVE-2017-10053 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10053

CVE-2017-10067 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10067

CVE-2017-10074 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10074

CVE-2017-10078 (CVE)
CVSS: Базовая оценка 5.5 (AV:N/AC:L/Au:S/C:P/I:P/A:N)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10078

CVE-2017-10081 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10081

CVE-2017-10087 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10087

CVE-2017-10089 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10089

CVE-2017-10090 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10090

CVE-2017-10096 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10096

CVE-2017-10101 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10101

CVE-2017-10102 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10102

CVE-2017-10107 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10107

CVE-2017-10108 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10108

CVE-2017-10109 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10109

CVE-2017-10110 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10110

CVE-2017-10111 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10111

CVE-2017-10115 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10115

CVE-2017-10116 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10116

CVE-2017-10135 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10135

CVE-2017-10193 (CVE)
CVSS: Базовая оценка 2.5 (AV:N/AC:H/Au:N/C:P/I:N/A:N)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10193

CVE-2017-10198 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10198

Обновление Риск: Высокий

ALTX ID 172709	**Обновление RHSA-2018:0151 : устранение уязвимостей и ошибок в kernel (важное)**

Описание

An industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization).

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18156
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18156

RHSA-2018:0151 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0151

CESA-2018:0151 (CESA-2018:0151)
http://lists.centos.org/pipermail/centos-announce/2018-January/022730.html

CVE-2015-8539 (CVE)
CVSS: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
CWE-264
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8539

CVE-2017-7472 (CVE)
CVSS: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)
CWE-399
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7472

CVE-2017-12192 (CVE)
CVSS: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)
CWE-476
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12192

CVE-2017-12193 (CVE)
CVSS: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)
CWE-476
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12193

CVE-2017-15649 (CVE)
CVSS: Базовая оценка 4.5 (AV:L/AC:L/Au:N/C:P/I:P/A:P)
CWE-362
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15649

Обновление Риск: Высокий

ALTX ID 172710	**Обновление RHSA-2018:0122 : устранение уязвимостей в firefox (критичное)**

Описание

This update upgrades Firefox to version 52.6.0 ESR.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18159
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18159

RHSA-2018:0122 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0122

CESA-2018:0122-CentOS 6 (CESA-2018:0122)
http://lists.centos.org/pipermail/centos-announce/2018-January/022716.html

CESA-2018:0122-CentOS 7 (CESA-2018:0122)
http://lists.centos.org/pipermail/centos-announce/2018-January/022717.html

CVE-2018-5089 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5089

CVE-2018-5091 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5091

CVE-2018-5095 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5095

CVE-2018-5096 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5096

CVE-2018-5097 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5097

CVE-2018-5098 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5098

CVE-2018-5099 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5099

CVE-2018-5102 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5102

CVE-2018-5103 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5103

CVE-2018-5104 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5104

CVE-2018-5117 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5117

Обновление Риск: Высокий

ALTX ID 172767	**Обновление RHSA-2017:3368 : устранение уязвимостей в qemu-kvm (умеренное)**

Описание

Quick Emulator (QEMU), compiled with the PC System Emulator with multiboot feature support, is vulnerable to an OOB r/w memory access issue. The issue could occur due to an integer overflow while loading a kernel image during a guest boot. A user or process could use this flaw to potentially achieve arbitrary code execution on a host. (CVE-2017-14167)
Quick emulator (QEMU), compiled with the Cirrus CLGD 54xx VGA Emulator support, is vulnerable to an OOB write access issue. The issue could occur while writing to VGA memory via mode4and5 write functions. A privileged user inside guest could use this flaw to crash the QEMU process resulting in Denial of Serivce (DoS). (CVE-2017-15289)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18421
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18421

BDU:2017-02299 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02299

RHSA-2017:3368 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:3368

CESA-2017:3368 (CESA-2017:3368)
http://lists.centos.org/pipermail/centos-announce/2017-December/022679.html

CVE-2017-14167 (CVE)
CVSS: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
CWE-787
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14167

CVE-2017-15289 (CVE)
CVSS: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:N/I:N/A:P)
CWE-787
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15289

Обновление Риск: Высокий

ALTX ID 172778	**Обновление RHSA-2017:3260 : устранение уязвимостей в samba (важное)**

Описание

A use-after-free flaw was found in the way samba servers handled certain SMB1 requests. An unauthenticated attacker could send

specially-crafted SMB1 requests to cause the server to crash or execute arbitrary code. (CVE-2017-14746)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18487
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18487

RHSA-2017:3260 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:3260

CESA-2017:3260 (CESA-2017:3260)
http://lists.centos.org/pipermail/centos-announce/2017-November/022631.html

CVE-2017-14746 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE-416
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14746

CVE-2017-15275 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15275

Обновление Риск: Высокий

ALTX ID 172779	**Обновление RHSA-2017:3247 : устранение уязвимостей в firefox (критичное)**

Описание

This update upgrades Firefox to version 52.5.0 ESR.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18488
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18488

RHSA-2017:3247 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:3247

CESA-2017:3247-CentOS 6 (CESA-2017:3247)
http://lists.centos.org/pipermail/centos-announce/2017-November/022627.html

CESA-2017:3247-CentOS 7 (CESA-2017:3247)
http://lists.centos.org/pipermail/centos-announce/2017-November/022628.html

CVE-2017-7826 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7826

CVE-2017-7828 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7828

CVE-2017-7830 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7830

Обновление Риск: Высокий

ALTX ID 172792	**Обновление RHSA-2017:3075 : устранение уязвимостей в wget (важное)**

Описание

A stack-based and a heap-based buffer overflow flaws were found in wget when processing chunked encoded HTTP responses. By tricking an unsuspecting user into connecting to a malicious HTTP server, an attacker could exploit these flaws to potentially execute arbitrary code. (CVE-2017-13089, CVE-2017-13090)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18532
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18532

BDU:2017-02577 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02577

BDU:2017-02576 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02576

RHSA-2017:3075 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:3075

CESA-2017:3075 (CESA-2017:3075)
http://lists.centos.org/pipermail/centos-announce/2017-October/022609.html

CVE-2017-13089 (CVE)
CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13089

CVE-2017-13090 (CVE)
CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13090

Обновление Риск: Высокий

ALTX ID 172799

Обновление RHSA-2017:2930 : устранение уязвимостей и ошибок в kernel (важное)

Описание

Out-of-bounds kernel heap access vulnerability was found in xfrm, kernel's IP framework for transforming packets. An error dealing with netlink messages from an unprivileged user leads to arbitrary read/write and privilege escalation. (CVE-2017-7184, Important)
A race condition issue leading to a use-after-free flaw was found in the way the raw packet sockets are implemented in the Linux kernel networking subsystem handling synchronization. A local user able to open a raw packet socket (requires the CAP_NET_RAW capability) could use this flaw to elevate their privileges on the system. (CVE-2017-1000111, Important)
An exploitable memory corruption flaw was found in the Linux kernel. The append path can be erroneously switched from UFO to non-UFO in ip_ufo_append_data() when building an UFO packet with MSG_MORE option. If unprivileged user namespaces are available, this flaw can be exploited to gain root privileges. (CVE-2017-1000112, Important)
A flaw was found in the Linux networking subsystem where a local attacker with CAP_NET_ADMIN capabilities could cause an out-of-bounds memory access by creating a smaller-than-expected ICMP header and sending to its destination via sendto(). (CVE-2016-8399, Moderate)
Kernel memory corruption due to a buffer overflow was found in brcmf_cfg80211_mgmt_tx() function in Linux kernels from v3.9-rc1 to v4.13-rc1. The vulnerability can be triggered by sending a crafted NL80211_CMD_FRAME packet via netlink. This flaw is unlikely to be triggered remotely as certain userspace code is needed for this. An unprivileged local user could use this flaw to induce kernel memory corruption on the system, leading to a crash. Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although it is unlikely. (CVE-2017-7541, Moderate)
An integer overflow vulnerability in ip6_find_1stfragopt() function was found. A local attacker that has privileges (of CAP_NET_RAW) to open raw socket can cause an infinite loop inside the ip6_find_1stfragopt() function. (CVE-2017-7542, Moderate)
A kernel data leak due to an out-of-bound read was found in the Linux kernel in inet_diag_msg_sctp{,l}addr_fill() and sctp_get_sctp_info() functions present since version 4.7-rc1 through version 4.13. A data leak happens when these functions fill in sockaddr data structures used to export socket's diagnostic information. As a result, up to 100 bytes of the slab data could be leaked to a userspace. (CVE-2017-7558, Moderate)

The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to possibly cause a situation where a value may be used after being freed (use-after-free) which may lead to memory corruption or other unspecified other impact. (CVE-2017-11176, Moderate)
A divide-by-zero vulnerability was found in the __tcp_select_window function in the Linux kernel. This can result in a kernel panic causing a local denial of service. (CVE-2017-14106, Moderate)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18553
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18553

BDU:2017-02488 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02488

BDU:2017-01686 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-01686

RHSA-2017:2930 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:2930

CESA-2017:2930 (CESA-2017:2930)
http://lists.centos.org/pipermail/centos-announce/2017-October/022605.html

CVE-2016-8399 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:H/Au:N/C:C/I:C/A:C)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8399

CVE-2017-1000111 (CVE)
CVSS: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
CWE-264
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000111

CVE-2017-1000112 (CVE)
CVSS: Базовая оценка 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)
CWE-362
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000112

CVE-2017-11176 (CVE)
CVSS: Базовая оценка 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
CWE-416
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11176

CVE-2017-14106 (CVE)
CVSS: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)
CWE-369
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14106

CVE-2017-7184 (CVE)
CVSS: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
CWE-264
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7184

CVE-2017-7541 (CVE)
CVSS: Базовая оценка 7.1 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7541

CVE-2017-7542 (CVE)
CVSS: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)
CWE-190
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7542

CVE-2017-7558 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7558

Обновление Риск: Высокий

ALTX ID 172813	**Обновление RHSA-2017:2836 : устранение уязвимостей в dnsmasq (критичное)**

Описание

A heap buffer overflow was found in dnsmasq in the code responsible for building DNS replies. An attacker could send crafted DNS packets to dnsmasq which would cause it to crash or, potentially, execute arbitrary code. (CVE-2017-14491)
A heap buffer overflow was discovered in dnsmasq in the IPv6 router advertisement (RA) handling code. An attacker on the local network segment could send crafted RAs to dnsmasq which would cause it to crash or, potentially, execute arbitrary code. This issue only affected configurations using one of these options: enable-ra, ra-only, slaac, ra-names, ra-advrouter, or ra-stateless. (CVE-2017-14492)
A stack buffer overflow was found in dnsmasq in the DHCPv6 code. An attacker on the local network could send a crafted DHCPv6 request to dnsmasq which would cause it to a crash or, potentially, execute arbitrary code. (CVE-2017-14493)
An information leak was found in dnsmasq in the DHCPv6 relay code. An attacker on the local network could send crafted DHCPv6 packets to dnsmasq causing it to forward the contents of process memory, potentially leaking sensitive data. (CVE-2017-14494)
A memory exhaustion flaw was found in dnsmasq in the EDNS0 code. An attacker could send crafted DNS packets which would trigger memory allocations which would never be freed, leading to unbounded memory consumption and eventually a crash. This issue only affected configurations using one of the options: add-mac, add-cpe-id, or add-subnet. (CVE-2017-14495)
An integer underflow flaw leading to a buffer over-read was found in dnsmasq in the EDNS0 code. An attacker could send crafted DNS packets to dnsmasq which would cause it to crash. This issue only affected configurations using one of the options: add-mac, add-cpe-id, or add-subnet. (CVE-2017-14496)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18618
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18618

BDU:2018-00110 (FSTEC)
http://www.bdu.fstec.ru/vul/2018-00110

BDU:2017-02360 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02360

BDU:2017-02359 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02359

BDU:2017-02358 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02358

BDU:2017-02357 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02357

RHSA-2017:2836 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:2836

CESA-2017:2836 (CESA-2017:2836)
http://lists.centos.org/pipermail/centos-announce/2017-October/022555.html

CVE-2017-14491 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14491

CVE-2017-14492 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14492

CVE-2017-14493 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14493

CVE-2017-14494 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE-200
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14494

CVE-2017-14495 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE-399
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14495

CVE-2017-14496 (CVE)
CVSS: Базовая оценка 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
CWE-191
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14496

Обновление Риск: Высокий

ALTX ID 172815	**Обновление RHSA-2017:2831 : устранение уязвимостей в firefox (критичное)**

Описание

This update upgrades Firefox to version 52.4.0 ESR.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18622
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18622

BDU:2018-00162 (FSTEC)
http://www.bdu.fstec.ru/vul/2018-00162

BDU:2018-00161 (FSTEC)
http://www.bdu.fstec.ru/vul/2018-00161

BDU:2018-00160 (FSTEC)
http://www.bdu.fstec.ru/vul/2018-00160

BDU:2018-00158 (FSTEC)
http://www.bdu.fstec.ru/vul/2018-00158

BDU:2018-00157 (FSTEC)
http://www.bdu.fstec.ru/vul/2018-00157

BDU:2018-00156 (FSTEC)
http://www.bdu.fstec.ru/vul/2018-00156

BDU:2018-00155 (FSTEC)
http://www.bdu.fstec.ru/vul/2018-00155

RHSA-2017:2831 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:2831

CESA-2017:2831-CentOS 6 (CESA-2017:2831)
http://lists.centos.org/pipermail/centos-announce/2017-September/022553.html

CESA-2017:2831-CentOS 7 (CESA-2017:2831)
http://lists.centos.org/pipermail/centos-announce/2017-September/022551.html

CVE-2017-7793 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7793

CVE-2017-7810 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7810

CVE-2017-7814 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7814

CVE-2017-7818 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7818

CVE-2017-7819 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7819

CVE-2017-7823 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7823

CVE-2017-7824 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7824

Обновление Риск: Высокий

ALTX ID 172830	**Обновление RHSA-2017:2788 : устранение уязвимостей в augeas (важное)**

Описание

A vulnerability was discovered in augeas affecting the handling of escaped strings. An attacker could send crafted strings that would cause the application using augeas to copy past the end of a buffer, leading to a crash or possible code execution. (CVE-2017-7555)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18664
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18664

BDU:2018-00104 (FSTEC)
http://www.bdu.fstec.ru/vul/2018-00104

RHSA-2017:2788 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:2788

CESA-2017:2788 (CESA-2017:2788)
http://lists.centos.org/pipermail/centos-announce/2017-September/022545.html

CVE-2017-7555 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7555

Обновление Риск: Высокий

ALTX ID 172845	**Обновление RHSA-2017:2679 : устранение уязвимостей в kernel (важное)**

Описание

A stack buffer overflow flaw was found in the way the Bluetooth subsystem of the Linux kernel processed pending L2CAP configuration responses from a client. On systems with the stack protection feature enabled in the kernel (CONFIG_CC_STACKPROTECTOR=y, which is enabled on all architectures other than s390x and ppc64[le]), an unauthenticated attacker able to initiate a connection to a system via Bluetooth could use this flaw to crash the system. Due to the nature of the stack protection feature, code execution cannot be fully ruled out, although we believe it is unlikely. On systems without the stack protection feature (ppc64[le]; the Bluetooth modules are not built on s390x), an unauthenticated attacker able to initiate a connection to a system via Bluetooth could use this flaw to remotely execute arbitrary code on the system with ring 0 (kernel) privileges. (CVE-2017-1000251, Important)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18706
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18706

BDU:2017-02053 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02053

RHSA-2017:2679 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:2679

CESA-2017:2679 (CESA-2017:2679)
http://lists.centos.org/pipermail/centos-announce/2017-September/022536.html

CVE-2017-1000251 (CVE)
CVSS: Базовая оценка 8.3 (AV:A/AC:L/Au:N/C:C/I:C/A:C)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000251

Обновление Риск: Высокий

ALTX ID 172929	**Обновление RHSA-2018:0527 : устранение уязвимостей в firefox (критичное)**

Описание

This update upgrades Firefox to version 52.7.0 ESR.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18829
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18829

RHSA-2018:0527 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0527

CESA-2018:0527 (CESA-2018:0527)
http://lists.centos.org/pipermail/centos-announce/2018-March/022804.html

CVE-2018-5125 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5125

CVE-2018-5127 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5127

CVE-2018-5129 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5129

CVE-2018-5130 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5130

CVE-2018-5131 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5131

CVE-2018-5144 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5144

CVE-2018-5145 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5145

Обновление Риск: Высокий

ALTX ID 173269	**Обновление RHSA-2018:0549 : устранение уязвимостей в firefox (критичное)**

Описание

This update upgrades Firefox to version 52.7.2 ESR.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18888
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18888

RHSA-2018:0549 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0549

CESA-2018:0549-CentOS 6 (CESA-2018:0549)
http://lists.centos.org/pipermail/centos-announce/2018-March/022807.html

CESA-2018:0549-CentOS 7 (CESA-2018:0549)
http://lists.centos.org/pipermail/centos-announce/2018-March/022808.html

CVE-2018-5146 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5146

Обновление Риск: Средний

ALTX ID 161434	**Обновление RHSA-2017:1208 : устранение уязвимостей в jasper (важное)**

Описание

Multiple flaws were found in the way JasPer decoded JPEG 2000 image files. A specially crafted file could cause an application using JasPer to crash or, possibly, execute arbitrary code.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:25529
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:25529

RHSA-2017:1208 (VENDOR)
https://rhn.redhat.com/errata/RHSA-2017-1208.html

CVE-2015-5203 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-415
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5203

CVE-2015-5221 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-416
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5221

CVE-2016-10248 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE-476
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10248

CVE-2016-10249 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-190
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10249

CVE-2016-10251 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-190
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10251

CVE-2016-1577 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1577

CVE-2016-1867 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1867

CVE-2016-2089 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-20
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2089

CVE-2016-2116 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-399
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2116

CVE-2016-8654 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8654

CVE-2016-8690 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-476
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8690

CVE-2016-8691 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-369
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8691

CVE-2016-8692 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-369
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8692

CVE-2016-8693 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-415
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8693

CVE-2016-8883 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-399
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8883

CVE-2016-8884 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-476
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8884

CVE-2016-8885 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-476
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8885

CVE-2016-9262 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-190
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9262

CVE-2016-9387 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-190
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9387

CVE-2016-9388 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9388

CVE-2016-9389 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9389

CVE-2016-9390 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-20
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9390

CVE-2016-9391 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9391

CVE-2016-9392 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9392

CVE-2016-9393 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9393

CVE-2016-9394 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-20
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9394

CVE-2016-9560 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9560

CVE-2016-9583 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9583

CVE-2016-9591 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9591

CVE-2016-9600 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9600

CESA-2017:1208-CentOS 6 (CESA-2017:1208)
http://lists.centos.org/pipermail/centos-announce/2017-May/022408.html

CESA-2017:1208-CentOS 7 (CESA-2017:1208)
http://lists.centos.org/pipermail/centos-announce/2017-May/022411.html

Обновление	Риск: Средний
ALTX ID 163880	**Обновление RHSA-2017:1680 : устранение уязвимостей и ошибок в bind (важное)**
Описание	

* A flaw was found in the way BIND handled TSIG authentication for dynamic updates. A remote attacker able to communicate with an authoritative BIND server could use this flaw to manipulate the contents of a zone, by forging a valid TSIG or SIG(0) signature for a dynamic update request. (CVE-2017-3143)

* A flaw was found in the way BIND handled TSIG authentication of AXFR requests. A remote attacker, able to communicate with an authoritative BIND server, could use this flaw to view the entire contents of a zone by sending a specially constructed request packet. (CVE-2017-3142)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:27953
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:27953

BDU:2018-00105 (FSTEC)
http://www.bdu.fstec.ru/vul/2018-00105

RHSA-2017:1680 (VENDOR)
https://rhn.redhat.com/errata/RHSA-2017-1680.html

CESA-2017:1680 (CESA-2017:1680)
http://lists.centos.org/pipermail/centos-announce/2017-July/022493.html

CVE-2017-3142 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3142

CVE-2017-3143 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3143

Обновление Риск: Средний

ALTX ID	**Обновление RHSA-2017:1793 : устранение уязвимостей в graphite2 (важное)**
164628	

Описание

Various vulnerabilities have been discovered in Graphite2. An attacker able to trick an unsuspecting user into opening specially crafted font files in an application using Graphite2 could exploit these flaws to disclose potentially sensitive memory, cause an application crash, or, possibly, execute arbitrary code.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:28338
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:28338

RHSA-2017:1793 (VENDOR)
https://rhn.redhat.com/errata/RHSA-2017-1793.html

CVE-2017-7771 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7771

CVE-2017-7772 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7772

CVE-2017-7773 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7773

CVE-2017-7774 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7774

CVE-2017-7775 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7775

CVE-2017-7776 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7776
CVE-2017-7777 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7777
CVE-2017-7778 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7778

Обновление Риск: Средний

ALTX ID 172679	**Обновление RHSA-2018:0483 : устранение уязвимостей в dhcp (важное)**

Описание

dhcp: Buffer overflow in dhclient possibly allowing code execution triggered by malicious server (CVE-2018-5732)
dhcp: Reference count overflow in dhcpd allows denial of service (CVE-2018-5733)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:17760
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:17760
RHSA-2018:0483 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0483
CESA-2018:0483 (CESA-2018:0483)
http://lists.centos.org/pipermail/centos-announce/2018-March/022792.html
CVE-2018-5732 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5732
CVE-2018-5733 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5733

Обновление Риск: Средний

ALTX ID 172683	**Обновление RHSA-2018:0418 : устранение уязвимостей в libreoffice (умеренное)**

Описание

libreoffice: Remote arbitrary file disclosure vulnerability via WEBSERVICE formula (CVE-2018-6871)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:17886
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:17886
RHSA-2018:0418 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0418
CESA-2018:0418 (CESA-2018:0418)
http://lists.centos.org/pipermail/centos-announce/2018-March/022770.html

CVE-2018-6871 (CVE)

CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE-255
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6871

Обновление Риск: Средний

ALTX ID 172685	**Обновление RHSA-2018:0395 : устранение уязвимостей и ошибок в kernel (важное)**

Описание

Kernel: KVM: MMU potential stack buffer overrun during page walks (CVE-2017-12188, Important)
Kernel: KVM: debug exception via syscall emulation (CVE-2017-7518, Moderate)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:17932
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:17932

RHSA-2018:0395 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0395

CESA-2018:0395 (CESA-2018:0395)
http://lists.centos.org/pipermail/centos-announce/2018-March/022768.html

CVE-2017-7518 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7518

CVE-2017-12188 (CVE)

CVSS: Базовая оценка 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)
CWE-22
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12188

Обновление Риск: Средний

ALTX ID 172694	**Обновление RHSA-2018:0350 : устранение уязвимостей в gcab (важное)**

Описание

gcab: Extracting malformed .cab files causes stack smashing potentially leading to arbitrary code execution (CVE-2018-5345)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18031
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18031

RHSA-2018:0350 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0350

CESA-2018:0350 (CESA-2018:0350)
http://lists.centos.org/pipermail/centos-announce/2018-February/022766.html

CVE-2018-5345 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5345

Обновление Риск: Средний

ALTX ID	Обновление RHSA-2018:0260 : устранение уязвимостей в systemd (умеренное)
172701	

Описание

A race condition was found in systemd. This could result in automount requests not being serviced and processes using them could hang, causing denial of service. (CVE-2018-1049)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18087
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18087

RHSA-2018:0260 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0260

CESA-2018:0260 (CESA-2018:0260)
http://lists.centos.org/pipermail/centos-announce/2018-February/022760.html

CVE-2018-1049 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-362
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1049

Обновление Риск: Средний

ALTX ID	Обновление RHSA-2018:0223 : устранение уязвимостей в nautilus (умеренное)
172703	

Описание

An untrusted .desktop file with executable permission set could choose its displayed name and icon, and execute commands without warning when opened by the user. An attacker could use this flaw to trick a user into opening a .desktop file disguised as a document, such as a PDF, and execute arbitrary commands. (CVE-2017-14604)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18108
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18108

RHSA-2018:0223 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0223

CESA-2018:0223 (CESA-2018:0223)
http://lists.centos.org/pipermail/centos-announce/2018-January/022734.html

CVE-2017-14604 (CVE)
CVSS: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:N/I:P/A:N)
CWE-20
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14604

Обновление Риск: Средний

ALTX ID	Обновление RHSA-2018:0158 : устранение уязвимостей в dhcp (умеренное)
172707	

Описание

It was found that the DHCP daemon did not properly clean up closed OMAPI connections in certain cases. A remote attacker able to connect to the OMAPI port could use this flaw to exhaust file descriptors in the DHCP daemon, leading to a denial of service in the OMAPI functionality. (CVE-2017-3144)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18152
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18152

RHSA-2018:0158 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0158

CESA-2018:0158 (CESA-2018:0158)
http://lists.centos.org/pipermail/centos-announce/2018-January/022725.html

CVE-2017-3144 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3144

Обновление Риск: Средний

ALTX ID 172721	**Обновление RHSA-2018:0102 : устранение уязвимостей в bind (важное)**

Описание

A use-after-free flaw leading to denial of service was found in the way BIND internally handled cleanup operations on upstream recursion fetch contexts. A remote attacker could potentially use this flaw to make named, acting as a DNSSEC validating resolver, exit unexpectedly with an assertion failure via a specially crafted DNS request. (CVE-2017-3145)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18231
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18231

RHSA-2018:0102 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0102

CESA-2018:0102 (CESA-2018:0102)
http://lists.centos.org/pipermail/centos-announce/2018-January/022715.html

CVE-2017-3145 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3145

Обновление Риск: Средний

ALTX ID 172723	**Обновление RHSA-2018:0095 : устранение уязвимостей в java-1.8.0-openjdk (важное)**

Описание

Multiple flaws were found in the Hotspot and AWT components of OpenJDK.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18246
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18246

https://ovaldb.altx-soft.ru/Definition.aspx?id=oval.ru.altx-soft.nix.def.10240

RHSA-2018:0095 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0095

CESA-2018:0095-CentOS 6 (CESA-2018:0095)
http://lists.centos.org/pipermail/centos-announce/2018-January/022712.html

CESA-2018:0095-CentOS 7 (CESA-2018:0095)
http://lists.centos.org/pipermail/centos-announce/2018-January/022713.html

CVE-2018-2579 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE-200
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2579

CVE-2018-2582 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2582

CVE-2018-2588 (CVE)
CVSS: Базовая оценка 4.0 (AV:N/AC:L/Au:S/C:P/I:N/A:N)
CWE-200
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2588

CVE-2018-2599 (CVE)
CVSS: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:N/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2599

CVE-2018-2602 (CVE)
CVSS: Базовая оценка 3.7 (AV:L/AC:H/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2602

CVE-2018-2603 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2603

CVE-2018-2618 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2618

CVE-2018-2629 (CVE)
CVSS: Базовая оценка 2.5 (AV:N/AC:H/Au:N/C:N/I:P/A:N)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2629

CVE-2018-2633 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2633

CVE-2018-2634 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE-200
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2634

CVE-2018-2637 (CVE)
CVSS: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:P/I:P/A:N)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2637

CVE-2018-2641 (CVE)
CVSS: Базовая оценка 2.5 (AV:N/AC:H/Au:N/C:N/I:P/A:N)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2641

CVE-2018-2663 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2663

CVE-2018-2677 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2677

CVE-2018-2678 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-2678

Обновление Риск: Средний

ALTX ID 172724	**Обновление RHSA-2018:0094 : устранение уязвимостей в linux-firmware (важное)**

Описание

This update supersedes microcode provided by Red Hat with the CVE-2017-5715 (“Spectre”) CPU branch injection vulnerability mitigation.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18261
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18261

RHSA-2018:0094 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0094

CESA-2018:0094 (CESA-2018:0094)
http://lists.centos.org/pipermail/centos-announce/2018-January/022711.html

Обновление Риск: Средний

ALTX ID 172725	**Обновление RHSA-2018:0093 : устранение уязвимостей в microcode_ctl (важное)**

Описание

This update supersedes microcode provided by Red Hat with the CVE-2017-5715 (“Spectre”) CPU branch injection vulnerability mitigation.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18267
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18267

RHSA-2018:0093 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0093

CESA-2018:0093-CentOS 6 (CESA-2018:0093)
http://lists.centos.org/pipermail/centos-announce/2018-January/022709.html
CESA-2018:0093-CentOS 7 (CESA-2018:0093)
http://lists.centos.org/pipermail/centos-announce/2018-January/022710.html

Обновление Риск: Средний

ALTX ID 172730	**Обновление RHSA-2018:0029 : устранение уязвимостей в libvirt (важное)**

Описание

An industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization).

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18293
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18293
RHSA-2018:0029 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0029
CESA-2018:0029 (CESA-2018:0029)
http://lists.centos.org/pipermail/centos-announce/2018-January/022704.html

Обновление Риск: Средний

ALTX ID 172743	**Обновление RHSA-2018:0023 : устранение уязвимостей в qemu-kvm (важное)**

Описание

An industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization).

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18348
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18348
RHSA-2018:0023 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0023
CESA-2018:0023 (CESA-2018:0023)
http://lists.centos.org/pipermail/centos-announce/2018-January/022705.html

Обновление Риск: Средний

ALTX ID 172750	**Обновление RHSA-2018:0014 : устранение уязвимостей в linux-firmware (важное)**

Описание

An industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization).

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18366
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18366

RHSA-2018:0014 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0014

CESA-2018:0014 (CESA-2018:0014)
http://lists.centos.org/pipermail/centos-announce/2018-January/022698.html

Обновление Риск: Средний

ALTX ID 172752

Обновление RHSA-2018:0012 : устранение уязвимостей в microcode_ctl (важное)

Описание

An industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization).

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18369
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18369

RHSA-2018:0012 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0012

CESA-2018:0012 (CESA-2018:0012)
http://lists.centos.org/pipermail/centos-announce/2018-January/022697.html

Обновление Риск: Средний

ALTX ID 172757

Обновление RHSA-2018:0007 : устранение уязвимостей в kernel (важное)

Описание

An industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization).

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18389
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18389

RHSA-2018:0007 (VENDOR)
https://access.redhat.com/errata/RHSA-2018:0007

CESA-2018:0007 (CESA-2018:0007)
http://lists.centos.org/pipermail/centos-announce/2018-January/022696.html

Обновление Риск: Средний

ALTX ID 172762	**Обновление RHSA-2017:3384 : устранение уязвимостей в liblouis (умеренное)**

Описание

A missing fix for one stack-based buffer overflow in findTable() for CVE-2014-8184 was discovered. An attacker could cause denial of service or potentially allow arbitrary code execution. (CVE-2017-15101)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18405
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18405

RHSA-2017:3384 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:3384

CESA-2017:3384 (CESA-2017:3384)
http://lists.centos.org/pipermail/centos-announce/2017-December/022684.html

CVE-2017-15101 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15101

Обновление Риск: Средний

ALTX ID 172763	**Обновление RHSA-2017:3382 : устранение уязвимостей в firefox (важное)**

Описание

This update upgrades Firefox to version 52.5.1 ESR.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18406
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18406

RHSA-2017:3382 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:3382

CESA-2017:3382-CentOS 7 (CESA-2017:3382)
http://lists.centos.org/pipermail/centos-announce/2017-December/022683.html

CESA-2017:3382-CentOS 6 (CESA-2017:3382)
http://lists.centos.org/pipermail/centos-announce/2017-December/022687.html

CVE-2017-7843 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7843

Обновление Риск: Средний

ALTX ID 172764	**Обновление RHSA-2017:3379 : устранение уязвимостей и ошибок в sssd (умеренное)**

Описание

It was found that sssd's sysdb_search_user_by_upn_res() function did not sanitize requests when querying its local cache and was vulnerable to injection. In a centralized login environment, if a password hash was locally cached for a given user, an authenticated attacker could use this flaw to retrieve it. (CVE-2017-12173)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18408
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18408

RHSA-2017:3379 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:3379

CESA-2017:3379 (CESA-2017:3379)
http://lists.centos.org/pipermail/centos-announce/2017-December/022685.html

CVE-2017-12173 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12173

Обновление Риск: Средний

ALTX ID 172777

Обновление RHSA-2017:3263 : устранение уязвимостей в curl (умеренное)

Описание

A buffer overrun flaw was found in the IMAP handler of libcurl. By tricking an unsuspecting user into connecting to a malicious IMAP server, an attacker could exploit this flaw to potentially cause information disclosure or crash the application. (CVE-2017-1000257)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18484
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18484

RHSA-2017:3263 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:3263

CESA-2017:3263 (CESA-2017:3263)
http://lists.centos.org/pipermail/centos-announce/2017-November/022630.html

CVE-2017-1000257 (CVE)
CVSS: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000257

Обновление Риск: Средний

ALTX ID 172787

Обновление RHSA-2017:3111 : устранение уязвимостей в liblouis (умеренное)

Описание

Multiple flaws were found in the processing of translation tables in liblouis. An attacker could crash or potentially execute arbitrary code using malicious translation tables. (CVE-2014-8184, CVE-2017-13738, CVE-2017-13740, CVE-2017-13741, CVE-2017-13742, CVE-2017-13743, CVE-2017-13744)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18517
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18517

RHSA-2017:3111 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:3111

CESA-2017:3111 (CESA-2017:3111)
http://lists.centos.org/pipermail/centos-announce/2017-November/022612.html

CVE-2014-8184 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8184

CVE-2017-13738 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-125
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13738

CVE-2017-13740 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13740

CVE-2017-13741 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-416
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13741

CVE-2017-13742 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13742

CVE-2017-13743 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13743

CVE-2017-13744 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-125
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13744

Обновление Риск: Средний

ALTX ID 172794	**Обновление RHSA-2017:2998 : устранение уязвимостей в java-1.8.0-openjdk (критичное)**

Описание

Multiple flaws were discovered in the RMI and Hotspot components in OpenJDK.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18541
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18541

RHSA-2017:2998 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:2998

CESA-2017:2998-CentOS 6 (CESA-2017:2998)
http://lists.centos.org/pipermail/centos-announce/2017-October/022571.html

CESA-2017:2998-CentOS 7 (CESA-2017:2998)
http://lists.centos.org/pipermail/centos-announce/2017-October/022603.html

CVE-2017-10274 (CVE)
CVSS: Базовая оценка 4.0 (AV:N/AC:H/Au:N/C:P/I:P/A:N)
CWE-284

ALTX ID 172801

Обновление RHSA-2017:2907 : устранение уязвимостей в wpa_supplicant (важное)

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10281

CVE-2017-10285 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10285

CVE-2017-10295 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10295

CVE-2017-10345 (CVE)
CVSS: Базовая оценка 2.5 (AV:N/AC:H/Au:N/C:N/I:N/A:P)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10345

CVE-2017-10346 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10346

CVE-2017-10347 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10347

CVE-2017-10348 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10348

CVE-2017-10349 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10349

CVE-2017-10350 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10350

CVE-2017-10355 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10355

CVE-2017-10356 (CVE)
CVSS: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)
CWE-200
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10356

CVE-2017-10357 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10357

CVE-2017-10388 (CVE)
CVSS: Базовая оценка 5.0 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
CWE-284
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10388

Обновление Риск: Средний

Описание

A new exploitation technique called key reinstallation attacks (KRACK) affecting WPA2 has been discovered. A remote attacker within Wi-Fi range could exploit these attacks to decrypt Wi-Fi traffic or possibly inject forged Wi-Fi packets by manipulating cryptographic handshakes used by the WPA2 protocol. (CVE-2017-13077, CVE-2017-13078, CVE-2017-13080, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18557
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18557

BDU:2017-02272 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02272

BDU:2017-02271 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02271

BDU:2017-02270 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02270

BDU:2017-02268 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02268

BDU:2017-02266 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02266

BDU:2017-02264 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02264

BDU:2017-02263 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02263

RHSA-2017:2907 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:2907

CESA-2017:2907 (CESA-2017:2907)
http://lists.centos.org/pipermail/centos-announce/2017-October/022569.html

CVE-2017-13077 (CVE)
CVSS: Базовая оценка 5.4 (AV:A/AC:M/Au:N/C:P/I:P/A:P)
CWE-254
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13077

CVE-2017-13078 (CVE)
CVSS: Базовая оценка 2.9 (AV:A/AC:M/Au:N/C:N/I:P/A:N)
CWE-254
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13078

CVE-2017-13080 (CVE)
CVSS: Базовая оценка 2.9 (AV:A/AC:M/Au:N/C:N/I:P/A:N)
CWE-254
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13080

CVE-2017-13082 (CVE)
CVSS: Базовая оценка 5.8 (AV:A/AC:L/Au:N/C:P/I:P/A:P)
CWE-254
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13082

CVE-2017-13086 (CVE)
CVSS: Базовая оценка 5.4 (AV:A/AC:M/Au:N/C:P/I:P/A:P)
CWE-254
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13086

CVE-2017-13087 (CVE)

CVSS: Базовая оценка 2.9 (AV:A/AC:M/Au:N/C:N/I:P/A:N)
CWE-254
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13087

CVE-2017-13088 (CVE)

CVSS: Базовая оценка 2.9 (AV:A/AC:M/Au:N/C:N/I:P/A:N)
CWE-254
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13088

Обновление Риск: Средний

ALTX ID	**Обновление RHSA-2017:2832 : устранение уязвимостей в nss (важное)**
172814	

Описание

A use-after-free flaw was found in the TLS 1.2 implementation in the NSS library when client authentication was used. A malicious client could use this flaw to cause an application compiled against NSS to crash or, potentially, execute arbitrary code with the permission of the user running the application. (CVE-2017-7805)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18621
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18621

RHSA-2017:2832 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:2832

CESA-2017:2832-CentOS 6 (CESA-2017:2832)
http://lists.centos.org/pipermail/centos-announce/2017-September/022552.html

CESA-2017:2832-CentOS 7 (CESA-2017:2832)
http://lists.centos.org/pipermail/centos-announce/2017-September/022550.html

CVE-2017-7805 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7805

Обновление Риск: Средний

ALTX ID	**Обновление RHSA-2017:2790 : устранение уязвимостей в samba (умеренное)**
172828	

Описание

It was found that samba did not enforce "SMB signing" when certain configuration options were enabled. A remote attacker could launch a man-in-the-middle attack and retrieve information in plain-text. (CVE-2017-12150)
A flaw was found in the way samba client used encryption with the max protocol set as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowing an attacker to read or alter the contents of the connection via a man-in-the-middle attack. (CVE-2017-12151)
An information leak flaw was found in the way SMB1 protocol was implemented by Samba. A malicious client could use this flaw to dump server memory contents to a file on the samba share or to a shared printer, though the exact area of server memory cannot be controlled by the attacker. (CVE-2017-12163)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18660
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18660

RHSA-2017:2790 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:2790
CESA-2017:2790 (CESA-2017:2790)
http://lists.centos.org/pipermail/centos-announce/2017-September/022546.html
CVE-2017-12150 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12150
CVE-2017-12151 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12151
CVE-2017-12163 (CVE)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12163

Обновление Риск: Средний

ALTX ID 172831	**Обновление RHSA-2017:2771 : устранение уязвимостей в emacs (важное)**

Описание

A command injection flaw within the Emacs "enriched mode" handling has been discovered. By tricking an unsuspecting user into opening a specially crafted file using Emacs, a remote attacker could exploit this flaw to execute arbitrary commands with the privileges of the Emacs user. (CVE-2017-14482)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18665
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18665
RHSA-2017:2771 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:2771
CESA-2017:2771 (CESA-2017:2771)
http://lists.centos.org/pipermail/centos-announce/2017-September/022541.html
CVE-2017-14482 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-77
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14482

Обновление Риск: Средний

ALTX ID 172852	**Обновление RHSA-2017:2551 : устранение уязвимостей в poppler (умеренное)**

Описание

A stack-based buffer overflow was found in the poppler library. An attacker could create a malicious PDF file that would cause applications that use poppler (such as Evince) to crash, or potentially execute arbitrary code when opened. (CVE-2017-9775)
An integer overflow leading to heap-based buffer overflow was found in the poppler library. An attacker could create a malicious PDF file that would cause applications that use poppler (such as Evince) to crash, or potentially execute arbitrary code when opened. (CVE-2017-9776)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18718
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18718

RHSA-2017:2551 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:2551

CESA-2017:2551 (CESA-2017:2551)
http://lists.centos.org/pipermail/centos-cr-announce/2017-August/004691.html

CVE-2017-9775 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE-119
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9775

CVE-2017-9776 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE-190
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9776

Обновление Риск: Средний

ALTX ID 172856	**Обновление RHSA-2017:2492 : устранение уязвимостей в xmlsec1 (умеренное)**

Описание

It was discovered xmlsec1's use of libxml2 inadvertently enabled external entity expansion (XXE) along with validation. An attacker could craft an XML file that would cause xmlsec1 to try and read local files or HTTP/FTP URLs, leading to information disclosure or denial of service. (CVE-2017-1000061)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18731
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18731

RHSA-2017:2492 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:2492

CESA-2017:2492 (CESA-2017:2492)
http://lists.centos.org/pipermail/centos-cr-announce/2017-August/004693.html

CVE-2017-1000061 (CVE)
CVSS: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:P/I:N/A:P)
CWE-611
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000061

Обновление Риск: Низкий

ALTX ID 172770	**Обновление RHSA-2017:3315 : устранение уязвимостей и ошибок в kernel (умеренное)**

Описание

It was found that the timer functionality in the Linux kernel ALSA subsystem is prone to a race condition between read and ioctl system call handlers, resulting in an uninitialized memory disclosure to user space. A local user could use this flaw to read information belonging to other users. (CVE-2017-1000380, Moderate)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18442
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18442

BDU:2018-00018 (FSTEC)
http://www.bdu.fstec.ru/vul/2018-00018

RHSA-2017:3315 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:3315

CESA-2017:3315 (CESA-2017:3315)
http://lists.centos.org/pipermail/centos-announce/2017-December/022682.html

CVE-2017-1000380 (CVE)
CVSS: Базовая оценка 2.0 (AV:L/AC:L/Au:N/C:P/I:N/A:N)
CWE-200
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000380

Обновление Риск: Низкий

ALTX ID 172841	**Обновление RHSA-2017:2685 : устранение уязвимостей в bluez (умеренное)**

Описание

An information-disclosure flaw was found in the bluetoothd implementation of the Service Discovery Protocol (SDP). A specially crafted Bluetooth device could, without prior pairing or user interaction, retrieve portions of the bluetoothd process memory, including potentially sensitive information such as Bluetooth encryption keys. (CVE-2017-1000250)

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:18695
https://ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:18695

BDU:2017-02054 (FSTEC)
http://www.bdu.fstec.ru/vul/2017-02054

RHSA-2017:2685 (VENDOR)
https://access.redhat.com/errata/RHSA-2017:2685

CESA-2017:2685-CentOS 6 (CESA-2017:2685)
http://lists.centos.org/pipermail/centos-announce/2017-September/022531.html

CESA-2017:2685-CentOS 7 (CESA-2017:2685)
http://lists.centos.org/pipermail/centos-announce/2017-September/022535.html

CVE-2017-1000250 (CVE)
CVSS: Базовая оценка 3.2 (AV:A/AC:L/Au:N/C:P/I:N/A:N)
CWE-200
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000250