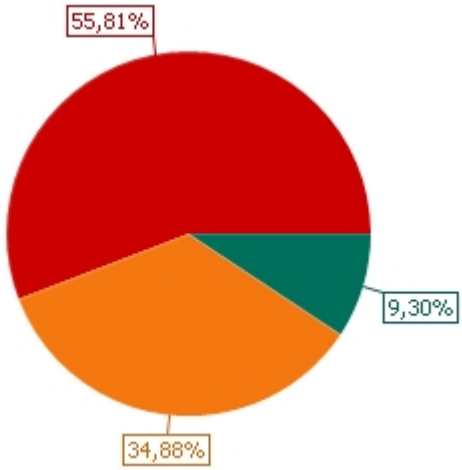
ALTEX SOFT

ОТЧЁТ

№ отчёта	*e050616d-8c18-499a-9263-2be585b4bd3c*
Профиль	*Обновления*
Задание	*Job_7964*
Начало/завершение сканирования	*19.05.2015 09:34:09 / 19.05.2015 09:34:37*
Формирование отчёта	*19.05.2015 15:37:13*
Имя	*Quick_192.168.100.101_187*
Описание	*Автогенерируемый отчет вкладки "История" для "192.168.100.101" из "Job_7964" задания.*
Хосты [1]	*192.168.100.101*

Диаграмма распределения обновлений по уровням риска



Риск	*Количество*
Высокий	*24*
Средний	*15*
Низкий	*4*
Всего	*43*

Таблица распределения обновлений по хостам

Хост / Риск	Высокий	Средний	Низкий	Всего
192.168.100.101	*24*	*15*	*4*	*43*
Всего	**24**	**15**	**4**	**43**

Таблица распределения обновлений по продуктам

Продукт / Риск	Высокий	Средний	Низкий	Всего
cpe:/o:ubuntu:ubuntu_linux:14.04	*24*	*15*	*4*	*43*
Всего	**24**	**15**	**4**	**43**

Хост: 192.168.100.101

CPE	*cpe:/o:ubuntu:ubuntu_linux:14.04*
Начало/завершение сканирования	*19.05.2015 09:34:09 / 19.05.2015 09:34:37*
Профиль	*Имя профиля: root* *Sudo: Нет*
Агент	*Нет*
Тип сканирования	*Полное*
Обновлений найдено	***43:*** ***24*** ***15*** ***4***

Обновления [43]

Хост	ALTX ID	Риск	Название
192.168.100.101	66725	Высокий	Обновление USN-2522-1 -- уязвимости ICU
cpe:/o:ubuntu:ubuntu_linux:14.04			*libicu52 (0:52.1-3)*
192.168.100.101	67258	Высокий	Обновление USN-2537-1 -- уязвимости OpenSSL
cpe:/o:ubuntu:ubuntu_linux:14.04			*libssl1.0.0 (0:1.0.1f-1ubuntu2.8)*
192.168.100.101	67051	Высокий	Обновление USN-2533-1 -- уязвимость Sudo
cpe:/o:ubuntu:ubuntu_linux:14.04			*sudo (0:1.8.9p5-1ubuntu1)*
192.168.100.101	69936	Высокий	Обновление USN-2570-1 -- уязвимости Oxide
cpe:/o:ubuntu:ubuntu_linux:14.04			*liboxideqtcore0 (0:1.4.3-0ubuntu0.14.04.1)* *oxideqt-codecs (0:1.4.3-0ubuntu0.14.04.1)*
192.168.100.101	69937	Высокий	Обновление USN-2580-1 -- уязвимости tcpdump
cpe:/o:ubuntu:ubuntu_linux:14.04			*tcpdump (0:4.5.1-2ubuntu1.1)*
192.168.100.101	66727	Высокий	Обновление USN-2505-2 -- регрессия Firefox
cpe:/o:ubuntu:ubuntu_linux:14.04			*firefox (0:36.0+build2-0ubuntu0.14.04.4)*
192.168.100.101	67050	Высокий	Обновление USN-2532-1 -- уязвимость cups-filters
cpe:/o:ubuntu:ubuntu_linux:14.04			*cups-browsed (0:1.0.52-0ubuntu1.2)*
192.168.100.101	66588	Высокий	Обновление USN-2506-1 -- уязвимости Thunderbird
cpe:/o:ubuntu:ubuntu_linux:14.04			*thunderbird (1:31.4.0+build1-0ubuntu0.14.04.1)*
192.168.100.101	66589	Высокий	Обновление USN-2516-3 -- регрессия Linux kernel vulnerabilities
cpe:/o:ubuntu:ubuntu_linux:14.04			*linux-image-3.13.0-46-generic (0:3.13.0-46.76)*
192.168.100.101	66780	Высокий	Обновление USN-2521-1 -- уязвимости Oxide
cpe:/o:ubuntu:ubuntu_linux:14.04			*liboxideqtcore0 (0:1.4.3-0ubuntu0.14.04.1)* *oxideqt-codecs (0:1.4.3-0ubuntu0.14.04.1)*
192.168.100.101	67054	Высокий	Обновление USN-2536-1 -- уязвимости libXfont
cpe:/o:ubuntu:ubuntu_linux:14.04			*libxfont1 (1:1.4.7-1ubuntu0.1)*
192.168.100.101	67259	Высокий	Обновление USN-2538-1 -- уязвимости Firefox
cpe:/o:ubuntu:ubuntu_linux:14.04			*firefox (0:36.0+build2-0ubuntu0.14.04.4)*
192.168.100.101	72043	Высокий	Обновление USN-2602-1 -- уязвимости Firefox
cpe:/o:ubuntu:ubuntu_linux:14.04			*firefox (0:36.0+build2-0ubuntu0.14.04.4)*
192.168.100.101	67442	Высокий	Обновление USN-2550-1 -- уязвимости Firefox
cpe:/o:ubuntu:ubuntu_linux:14.04			*firefox (0:36.0+build2-0ubuntu0.14.04.4)*
192.168.100.101	67445	Высокий	Обновление USN-2552-1 -- уязвимости Thunderbird
cpe:/o:ubuntu:ubuntu_linux:14.04			*thunderbird (1:31.4.0+build1-0ubuntu0.14.04.1)*
192.168.100.101	68521	Высокий	USN-2568-1 -- libx11, libxrender vulnerability
cpe:/o:ubuntu:ubuntu_linux:14.04			*libxrender1 (1:0.9.8-1)*

192.168.100.101	68523	Высокий	USN-2569-1 -- Apport vulnerability
cpe:/o:ubuntu:ubuntu_linux:14.04			*apport (0:2.14.1-0ubuntu3.7)*
192.168.100.101	69552	Высокий	Обновление USN-2572-1 -- уязвимости PHP
cpe:/o:ubuntu:ubuntu_linux:14.04			*php5-cli (0:5.5.9+dfsg-1ubuntu4.7)*
			libapache2-mod-php5 (0:5.5.9+dfsg-1ubuntu4.7)
192.168.100.101	70999	Высокий	Обновление USN-2604-1 -- уязвимость Libtasn1
cpe:/o:ubuntu:ubuntu_linux:14.04			*libtasn1-6 (0:3.4-3ubuntu0.1)*
192.168.100.101	69939	Высокий	Обновление USN-2578-1 -- уязвимости LibreOffice
cpe:/o:ubuntu:ubuntu_linux:14.04			*libreoffice-core (1:4.2.7-0ubuntu2)*
192.168.100.101	69754	Высокий	Обновление USN-2574-1 -- уязвимости OpenJDK 7
cpe:/o:ubuntu:ubuntu_linux:14.04			*openjdk-7-jre-headless (0:7u75-2.5.4-1~trusty1)*
192.168.100.101	67490	Высокий	Обновление USN-2556-1 -- уязвимости Oxide
cpe:/o:ubuntu:ubuntu_linux:14.04			*liboxideqtcore0 (0:1.4.3-0ubuntu0.14.04.1)*
192.168.100.101	70974	Высокий	Обновление USN-2591-1 -- уязвимости curl
cpe:/o:ubuntu:ubuntu_linux:14.04			*libcurl3-gnutls (0:7.35.0-1ubuntu2.3)*
			libcurl3 (0:7.35.0-1ubuntu2.3)
192.168.100.101	70987	Высокий	Обновление USN-2582-1 -- уязвимости Oxide
cpe:/o:ubuntu:ubuntu_linux:14.04			*liboxideqtcore0 (0:1.4.3-0ubuntu0.14.04.1)*
192.168.100.101	67317	Средний	Обновление USN-2540-1 -- уязвимости GnuTLS
cpe:/o:ubuntu:ubuntu_linux:14.04			*libgnutls26 (0:2.12.23-12ubuntu2.1)*
192.168.100.101	67443	Средний	Обновление USN-2555-1 -- уязвимости Libgcrypt
cpe:/o:ubuntu:ubuntu_linux:14.04			*libgcrypt11 (0:1.5.3-2ubuntu4.1)*
192.168.100.101	67319	Средний	Обновление USN-2549-1 -- уязвимости libarchive
cpe:/o:ubuntu:ubuntu_linux:14.04			*libarchive13 (0:3.1.2-7ubuntu2)*
192.168.100.101	68482	Средний	Обновление USN-2566-1 -- уязвимость dpkg
cpe:/o:ubuntu:ubuntu_linux:14.04			*libdpkg-perl (0:1.17.5ubuntu5.3-0)*
192.168.100.101	67052	Средний	Обновление USN-2531-1 -- уязвимость Requests
cpe:/o:ubuntu:ubuntu_linux:14.04			*python3-requests (0:2.2.1-1ubuntu0.1)*
			python-requests (0:2.2.1-1ubuntu0.1)
192.168.100.101	69756	Средний	Обновление USN-2577-1 -- уязвимость wpa_supplicant
cpe:/o:ubuntu:ubuntu_linux:14.04			*wpasupplicant (0:2.1-0ubuntu1.1)*
192.168.100.101	67441	Средний	Обновление USN-2553-1 -- уязвимости LibTIFF
cpe:/o:ubuntu:ubuntu_linux:14.04			*libtiff5 (0:4.0.3-7ubuntu0.1)*
192.168.100.101	67446	Средний	Обновление USN-2553-2 -- регрессия LibTIFF
cpe:/o:ubuntu:ubuntu_linux:14.04			*libtiff5 (0:4.0.3-7ubuntu0.1)*
192.168.100.101	66786	Средний	Обновление USN-2528-1 -- уязвимость Linux kernel
cpe:/o:ubuntu:ubuntu_linux:14.04			*linux-image-3.13.0-46-generic (0:3.13.0-46.76)*
192.168.100.101	69935	Средний	Обновление USN-2581-1 -- уязвимость NetworkManager
cpe:/o:ubuntu:ubuntu_linux:14.04			*network-manager (0:0.9.8.8-0ubuntu7)*
192.168.100.101	69759	Средний	Обновление USN-2571-1 -- уязвимость Firefox
cpe:/o:ubuntu:ubuntu_linux:14.04			*firefox (0:36.0+build2-0ubuntu0.14.04.4)*
192.168.100.101	70983	Средний	Обновление USN-2593-1 -- уязвимость Dnsmasq
cpe:/o:ubuntu:ubuntu_linux:14.04			*dnsmasq-base (0:2.68-1)*
192.168.100.101	69758	Средний	Обновление USN-2576-1 -- уязвимость usb-creator
cpe:/o:ubuntu:ubuntu_linux:14.04			*usb-creator-common (0:0.2.56.3-0)*
192.168.100.101	67491	Средний	Обновление USN-2557-1 -- уязвимость Firefox
cpe:/o:ubuntu:ubuntu_linux:14.04			*firefox (0:36.0+build2-0ubuntu0.14.04.4)*

192.168.100.101	70984	Средний	Обновление USN-2595-1 -- уязвимость ppp
cpe:/o:ubuntu:ubuntu_linux:14.04			*ppp (0:2.4.5-5.1ubuntu2.1)*
192.168.100.101	69551	Низкий	Обновление USN-2569-2 -- уязвимость Apport
cpe:/o:ubuntu:ubuntu_linux:14.04			*apport (0:2.14.1-0ubuntu3.7)*
192.168.100.101	67444	Низкий	Обновление USN-2554-1 -- уязвимости GnuPG
cpe:/o:ubuntu:ubuntu_linux:14.04			*gnupg (0:1.4.16-1ubuntu2.1)*
192.168.100.101	67492	Низкий	Обновление USN-2559-1 -- уязвимость Libtasn1
cpe:/o:ubuntu:ubuntu_linux:14.04			*libtasn1-6 (0:3.4-3ubuntu0.1)*
192.168.100.101	70998	Низкий	Обновление USN-2605-1 -- уязвимости ICU
cpe:/o:ubuntu:ubuntu_linux:14.04			*libicu52 (0:52.1-3)*

Список обновлений

Обновление Риск: Высокий

ALTX ID 68521	**USN-2568-1 -- libx11, libxrender vulnerability**

Описание

Abhishek Arya discovered that libX11 incorrectly handled memory in the MakeBigReq macro. A remote attacker could use this issue to cause applications to crash, resulting in a denial of service, or possibly execute arbitrary code.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7789
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7789

USN-2568-1 (VENDOR)
USN-2568-1

CVE-2013-7439 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-189
CVE-2013-7439

Обновление Риск: Высокий

ALTX ID 68523	**USN-2569-1 -- Apport vulnerability**

Описание

StГ©phane Graber and Tavis Ormandy independently discovered that Apport incorrectly handled the crash reporting feature. A local attacker could use this issue to gain elevated privileges.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7791
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7791

USN-2569-1 (VENDOR)
USN-2569-1

CVE-2015-1318 (CVE)
CVSS: Базовая оценка 7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
CWE: CWE-264
CVE-2015-1318

Обновление Риск: Высокий

ALTX ID 69552	**Обновление USN-2572-1 -- уязвимости PHP**

Описание

It was discovered that PHP incorrectly handled cleanup when used with Apache 2.4. A remote attacker could use this issue to cause PHP to crash, resulting in a denial of service, or possibly execute arbitrary code.

It was discovered that PHP incorrectly handled opening tar, zip or phar archives through the PHAR extension. A remote attacker could use this issue to cause PHP to crash, resulting in a denial of service, or possibly execute arbitrary code.

It was discovered that PHP incorrectly handled regular expressions. A remote attacker could use this issue to cause PHP to crash, resulting in a denial of service, or possibly execute arbitrary code.

Paulos Yibelo discovered that PHP incorrectly handled moving files when a pathname contained a null character. A remote attacker could use this issue to possibly bypass filename restrictions. This issue only applied to Ubuntu 14.04 LTS and Ubuntu 14.10.

It was discovered that PHP incorrectly handled unserializing PHAR files. A remote attacker could use this issue to cause PHP to possibly expose sensitive information.

Taoguang Chen discovered that PHP incorrectly handled unserializing certain objects. A remote attacker could use this issue to cause PHP to crash, resulting in a denial of service, or possibly execute arbitrary code.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7798
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7798

USN-2572-1 (VENDOR)
USN-2572-1

CVE-2015-3330 (CVE)
CVE-2015-3330

CVE-2015-3329 (CVE)
CVE-2015-3329

CVE-2015-2305 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-189
CVE-2015-2305

CVE-2015-2348 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-264
CVE-2015-2348

CVE-2015-2783 (CVE)
CVE-2015-2783

CVE-2015-2787 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-2787

Обновление Риск: Высокий

ALTX ID 72043	**Обновление USN-2602-1 -- уязвимости Firefox**

Описание

Jesse Ruderman, Mats Palmgren, Byron Campen, Steve Fink, Gary Kwong, Andrew McCreight, Christian Holler, Jon Coppeard, and Milan Sreckovic discovered multiple memory safety issues in Firefox. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox.

Atte Kettunen discovered a buffer overflow during the rendering of SVG content with certain CSS properties in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox.

Alex Verstak discovered that <meta name="referrer"> is ignored in some circumstances.

Dougall Johnson discovered an out of bounds read and write in asm.js. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to obtain sensitive information, cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox.

Scott Bell discovered a use-afer-free during the processing of text when vertical text is enabled. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox.

Tyson Smith and Jesse Schwartzentruber discovered a use-after-free during shutdown. An attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox.

Ucha Gobejishvili discovered a buffer overflow when parsing compressed XML content. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox.

A buffer overflow and out-of-bounds read were discovered when parsing metadata in MP4 files in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Firefox.

Mark Hammond discovered that when a trusted page is hosted within an iframe in an untrusted page, the untrusted page can intercept webchannel responses meant for the trusted page in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could exploit this to bypass origin restrictions.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7925

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7925

USN-2602-1 (VENDOR)

USN-2602-1

CVE-2015-2708 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-2708

CVE-2015-2709 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-2709

CVE-2015-2710 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-119
CVE-2015-2710

CVE-2015-2711 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE: CWE-200
CVE-2015-2711

CVE-2015-2712 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-119
CVE-2015-2712

CVE-2015-2713 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVE-2015-2713

CVE-2015-2715 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-362
CVE-2015-2715

CVE-2015-2716 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-119
CVE-2015-2716

CVE-2015-2717 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-189
CVE-2015-2717

CVE-2015-2718 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE: CWE-200
CVE-2015-2718

Обновление Риск: Высокий

ALTX ID 67442	**Обновление USN-2550-1 -- уязвимости Firefox**

Описание

Olli Pettay and Boris Zbarsky discovered an issue during anchor navigations in some circumstances. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to bypass same-origin policy restrictions.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7726

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7726

USN-2550-1 (VENDOR)

USN-2550-1

CVE-2015-0801 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-264
CVE-2015-0801

CVE-2015-0802 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-264
CVE-2015-0802

CVE-2015-0803 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-264
CVE-2015-0803

CVE-2015-0804 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-264
CVE-2015-0804

CVE-2015-0805 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-17
CVE-2015-0805

CVE-2015-0806 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-17
CVE-2015-0806

CVE-2015-0807 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-352
CVE-2015-0807

CVE-2015-0808 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-17
CVE-2015-0808

CVE-2015-0811 (CVE)

CVSS: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P)
CWE: CWE-119
CVE-2015-0811

CVE-2015-0812 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-17
CVE-2015-0812

CVE-2015-0813 (CVE)

CVSS: Базовая оценка 5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
CVE-2015-0813

CVE-2015-0814 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-0814

CVE-2015-0815 (CVE)

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

CVE-2015-0815

CVE-2015-0816 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)

CWE: CWE-264

CVE-2015-0816

Обновление Риск: Высокий

ALTX ID 67445	**Обновление USN-2552-1 -- уязвимости Thunderbird**

Описание

Olli Pettay and Boris Zbarsky discovered an issue during anchor navigations in some circumstances. If a user were tricked in to opening a specially crafted message with scripting enabled, an attacker could potentially exploit this to bypass same-origin policy restrictions.

Christoph Kerschbaumer discovered that CORS requests from navigator.sendBeacon() followed 30x redirections after preflight. If a user were tricked in to opening a specially crafted message with scripting enabled, an attacker could potentially exploit this to conduct cross-site request forgery (XSRF) attacks.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7729

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7729

USN-2552-1 (VENDOR)

USN-2552-1

CVE-2015-0801 (CVE)

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

CWE: CWE-264

CVE-2015-0801

CVE-2015-0807 (CVE)

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

CWE: CWE-352

CVE-2015-0807

CVE-2015-0813 (CVE)

CVSS: Базовая оценка 5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVE-2015-0813

CVE-2015-0815 (CVE)

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

CVE-2015-0815

CVE-2015-0816 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)

CWE: CWE-264

CVE-2015-0816

Обновление Риск: Высокий

ALTX ID 67490	**Обновление USN-2556-1 -- уязвимости Oxide**

Описание

It was discovered that Chromium did not properly handle the interaction of IPC, the gamepad API and V8. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to execute arbitrary code with the privileges of the user invoking the program.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7752

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7752

USN-2556-1 (VENDOR)

USN-2556-1

CVE-2015-1233 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-17
CVE-2015-1233

CVE-2015-1234 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-362
CVE-2015-1234

CVE-2015-1317 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-1317

Обновление Риск: Высокий

ALTX ID 70974	**Обновление USN-2591-1 -- уязвимости curl**

Описание

Paras Sethia discovered that curl could incorrectly re-use NTLM HTTP credentials when subsequently connecting to the same host over HTTP.

Hanno BГ¶ck discovered that curl incorrectly handled zero-length host names. If a user or automated system were tricked into using a specially crafted host name, an attacker could possibly use this issue to cause curl to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 14.10 and Ubuntu 15.04.

Hanno BГ¶ck discovered that curl incorrectly handled cookie path elements. If a user or automated system were tricked into parsing a specially crafted cookie, an attacker could possibly use this issue to cause curl to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 14.04 LTS, Ubuntu 14.10 and Ubuntu 15.04.

Isaac Boukris discovered that when using Negotiate authenticated connections, curl could incorrectly authenticate the entire connection and not just specific HTTP requests.

Yehezkel Horowitz and Oren Souroujon discovered that curl sent HTTP headers

both to servers and proxies by default, contrary to expectations. This issue only affected Ubuntu 14.10 and Ubuntu 15.04.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7865
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7865

USN-2591-1 (VENDOR)
USN-2591-1

CVE-2015-3143 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-264
CVE-2015-3143

CVE-2015-3144 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-119
CVE-2015-3144

CVE-2015-3145 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-119
CVE-2015-3145

CVE-2015-3148 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-284
CVE-2015-3148

CVE-2015-3153 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-200
CVE-2015-3153

Обновление Риск: Высокий

ALTX ID 70987	**Обновление USN-2582-1 -- уязвимости Oxide**

Описание

A use-after-free was discovered in the DOM implementation in Blink. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via renderer crash, or execute arbitrary code with the privileges of the sandboxed render process.

Multiple security issues were discovered in Chromium. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to read uninitialized memory, cause a denial of service via application crash or execute arbitrary code with the privileges of the user invoking the program.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7878
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7878

USN-2582-1 (VENDOR)

USN-2582-1

CVE-2015-1243 (CVE)

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

CVE-2015-1243

CVE-2015-1250 (CVE)

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

CVE-2015-1250

Обновление Риск: Высокий

ALTX ID 70999	**Обновление USN-2604-1 -- уязвимость Libtasn1**

Описание

Hanno ВГ¶ck discovered that Libtasn1 incorrectly handled certain ASN.1 data. A remote attacker could possibly exploit this with specially crafted ASN.1 data and cause applications using Libtasn1 to crash, resulting in a denial of service, or possibly execute arbitrary code.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7890

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7890

USN-2604-1 (VENDOR)

USN-2604-1

CVE-2015-3622 (CVE)

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

CWE: CWE-119

CVE-2015-3622

Обновление Риск: Высокий

ALTX ID 69939	**Обновление USN-2578-1 -- уязвимости LibreOffice**

Описание

Alexander Cherepanov discovered that LibreOffice incorrectly handled certain RTF files. If a user were tricked into opening a specially crafted RTF document, a remote attacker could cause LibreOffice to crash, and possibly execute arbitrary code.

It was discovered that LibreOffice incorrectly handled certain HWP files. If a user were tricked into opening a specially crafted HWP document, a remote attacker could cause LibreOffice to crash, and possibly execute arbitrary code.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7841

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7841

USN-2578-1 (VENDOR)

USN-2578-1

CVE-2014-9093 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-20
CVE-2014-9093

CVE-2015-1774 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-119
CVE-2015-1774

Обновление Риск: Высокий

ALTX ID 69754	**Обновление USN-2574-1 -- уязвимости OpenJDK 7**

Описание

Several vulnerabilities were discovered in the OpenJDK JRE related to information disclosure, data integrity and availability. An attacker could exploit these to cause a denial of service or expose sensitive data over the network.

Alexander Cherepanov discovered that OpenJDK JRE was vulnerable to directory traversal issues with respect to handling jar files. An attacker could use this to expose sensitive data.

Florian Weimer discovered that the RSA implementation in the JCE component in OpenJDK JRE did not follow recommended practices for implementing RSA signatures. An attacker could use this to expose sensitive data.

A vulnerability was discovered in the OpenJDK JRE related to data integrity. An attacker could exploit this expose sensitive data over the network.

A vulnerability was discovered in the OpenJDK JRE related to availability. An attacker could exploit these to cause a denial of service.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7820

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7820

USN-2574-1 (VENDOR)

USN-2574-1

CVE-2015-0460 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
CVE-2015-0460

CVE-2015-0469 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVE-2015-0469

CVE-2015-0480 (CVE)

CVSS: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:N/I:P/A:P)
CVE-2015-0480

CVE-2015-0478 (CVE)

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

CVE-2015-0478

CVE-2015-0477 (CVE)

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

CVE-2015-0477

CVE-2015-0488 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVE-2015-0488

Обновление	Риск: Высокий
ALTX ID 69936	**Обновление USN-2570-1 -- уязвимости Oxide**

Описание

An issue was discovered in the HTML parser in Blink. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to bypass same-origin restrictions.

An issue was discovered in the Web Audio API implementation in Blink. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to bypass same-origin restrictions.

A use-after-free was discovered in Chromium. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via renderer crash, or execute arbitrary code with the privileges of the sandboxed render process.

An out-of-bounds write was discovered in Skia. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash or execute arbitrary code with the privileges of the user invoking the program.

An out-of-bounds read was discovered in the WebGL implementation. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via renderer crash.

An issue was discovered with the interaction of page navigation and touch event handling. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to conduct "tap jacking" attacks.

A type confusion bug was discovered in V8. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via renderer crash, or execute arbitrary code with the privileges of the sandboxed render process.

It was discovered that websocket connections were not upgraded whenever a HSTS policy is active. A remote attacker could potentially exploit this to conduct a man in the middle (MITM) attack.

An out-of-bounds read was discovered in Blink. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via renderer crash.

Multiple security issues were discovered in Chromium. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to read uninitialized memory, cause a denial of service via application crash or execute arbitrary code with the

privileges of the user invoking the program.

A use-after-free was discovered in the file picker implementation. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit this to cause a denial of service via application crash or execute arbitrary code with the privileges of the user invoking the program.

Multiple security issues were discovered in V8. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to read uninitialized memory, cause a denial of service via renderer crash or execute arbitrary code with the privileges of the sandboxed render process.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7838

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7838

USN-2570-1 (VENDOR)

USN-2570-1

CVE-2015-1235 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-264
CVE-2015-1235

CVE-2015-1236 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE: CWE-264
CVE-2015-1236

CVE-2015-1237 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-1237

CVE-2015-1238 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-119
CVE-2015-1238

CVE-2015-1240 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-119
CVE-2015-1240

CVE-2015-1241 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-20
CVE-2015-1241

CVE-2015-1242 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-1242

CVE-2015-1244 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-200
CVE-2015-1244

CVE-2015-1246 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-119
CVE-2015-1246

CVE-2015-1249 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-1249

CVE-2015-1321 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVE-2015-1321

CVE-2015-3333 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-3333

Обновление Риск: Высокий

ALTX ID 69937	**Обновление USN-2580-1 -- уязвимости tcpdump**

Описание

It was discovered that tcpdump incorrectly handled printing certain packets. A remote attacker could use this issue to cause tcpdump to crash, resulting in a denial of service, or possibly execute arbitrary code.

In the default installation, attackers would be isolated by the tcpdump AppArmor profile.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7839
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7839

USN-2580-1 (VENDOR)
USN-2580-1

CVE-2015-0261 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-189
CVE-2015-0261

CVE-2015-2153 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-119
CVE-2015-2153

CVE-2015-2154 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-119
CVE-2015-2154

CVE-2015-2155 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-2155

Обновление Риск: Высокий

ALTX ID 66727	**Обновление USN-2505-2 -- регрессия Firefox**

Описание

USN-2505-1 fixed vulnerabilities in Firefox. This update removed the deprecated "-remote" command-line switch that some older software still depends on. This update fixes the problem.

We apologize for the inconvenience.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7560

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7560

USN-2505-2 (VENDOR)

USN-2505-2

CVE-2015-0819 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-19
CVE-2015-0819

CVE-2015-0820 (CVE)

CVSS: Базовая оценка 2.6 (AV:N/AC:H/Au:N/C:N/I:P/A:N)
CWE: CWE-284
CVE-2015-0820

CVE-2015-0821 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-264
CVE-2015-0821

CVE-2015-0822 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE: CWE-200
CVE-2015-0822

CVE-2015-0823 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-0823

CVE-2015-0824 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-119
CVE-2015-0824

CVE-2015-0825 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE: CWE-119
CVE-2015-0825

CVE-2015-0826 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-119
CVE-2015-0826

CVE-2015-0827 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE: CWE-119
CVE-2015-0827

CVE-2015-0829 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-119
CVE-2015-0829

CVE-2015-0830 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-399
CVE-2015-0830

CVE-2015-0831 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVE-2015-0831

CVE-2015-0832 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-254
CVE-2015-0832

CVE-2015-0834 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE: CWE-200
CVE-2015-0834

CVE-2015-0835 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-0835

CVE-2015-0836 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-0836

Обновление Риск: Высокий

ALTX ID 66725	**Обновление USN-2522-1 -- уязвимости ICU**

Описание

It was discovered that ICU incorrectly handled memory operations when processing fonts. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program. This issue only affected Ubuntu 12.04 LTS.

It was discovered that ICU incorrectly handled memory operations when processing fonts. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program.

It was discovered that ICU incorrectly handled memory operations when processing regular expressions. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program.

It was discovered that ICU collator implementation incorrectly handled memory operations. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7558
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7558

USN-2522-1 (VENDOR)
USN-2522-1

CVE-2013-1569 (CVE)
CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVE-2013-1569

CVE-2013-2383 (CVE)
CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVE-2013-2383

CVE-2013-2384 (CVE)
CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVE-2013-2384

CVE-2013-2419 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVE-2013-2419

CVE-2014-6585 (CVE)
CVSS: Базовая оценка 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVE-2014-6585

CVE-2014-6591 (CVE)
CVSS: Базовая оценка 2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)
CVE-2014-6591

CVE-2014-7923 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-17
CVE-2014-7923

CVE-2014-7926 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-17
CVE-2014-7926

CVE-2014-9654 (CVE)
CVE-2014-9654

CVE-2014-7940 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-399
CVE-2014-7940

Обновление	Риск: Высокий
ALTX ID 67258	**Обновление USN-2537-1 -- уязвимости OpenSSL**

Описание

It was discovered that OpenSSL incorrectly handled malformed EC private key files. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service, or execute arbitrary code.

Stephen Henson discovered that OpenSSL incorrectly handled comparing ASN.1 boolean types. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service.

Emilia KГ¤sper discovered that OpenSSL incorrectly handled ASN.1 structure reuse. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service, or execute arbitrary code.

Brian Carpenter discovered that OpenSSL incorrectly handled invalid certificate keys. A remote attacker could possibly use this issue to cause

OpenSSL to crash, resulting in a denial of service.

Michal Zalewski discovered that OpenSSL incorrectly handled missing outer ContentInfo when parsing PKCS#7 structures. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service, or execute arbitrary code.

Robert Dugal and David Ramos discovered that OpenSSL incorrectly handled decoding Base64 encoded data. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service, or execute arbitrary code.

Sean Burford and Emilia KГ¤sper discovered that OpenSSL incorrectly handled specially crafted SSLv2 CLIENT-MASTER-KEY messages. A remote attacker could possibly use this issue to cause OpenSSL to crash, resulting in a denial of service.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7650
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7650

USN-2537-1 (VENDOR)
USN-2537-1

CVE-2015-0209 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVE-2015-0209

CVE-2015-0286 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-17
CVE-2015-0286

CVE-2015-0287 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-17
CVE-2015-0287

CVE-2015-0288 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVE-2015-0288

CVE-2015-0289 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CVE-2015-0289

CVE-2015-0292 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-119
CVE-2015-0292

CVE-2015-0293 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-20
CVE-2015-0293

Обновление Риск: Высокий

ALTX ID 67051	**Обновление USN-2533-1 -- уязвимость Sudo**

Описание

Jakub Wilk and Stephane Chazelas discovered that Sudo incorrectly handled the TZ environment variable. An attacker with Sudo access could possibly use this issue to open arbitrary files, bypassing intended permissions.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7629

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7629

USN-2533-1 (VENDOR)

USN-2533-1

CVE-2014-9680 (CVE)

CVE-2014-9680

Обновление Риск: Высокий

ALTX ID 66780	**Обновление USN-2521-1 -- уязвимости Oxide**

Описание

Several out-of-bounds write bugs were discovered in Skia. If a user were tricked in to opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service via application crash or execute arbitrary code with the privileges of the user invoking the program.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7588

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7588

USN-2521-1 (VENDOR)

USN-2521-1

CVE-2015-1213 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-119
CVE-2015-1213

CVE-2015-1214 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-189
CVE-2015-1214

CVE-2015-1215 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-119
CVE-2015-1215

CVE-2015-1216 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-1216

CVE-2015-1217 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-17
CVE-2015-1217

CVE-2015-1230 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-1230

CVE-2015-1218 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-1218

CVE-2015-1223 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-1223

CVE-2015-1219 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-189
CVE-2015-1219

CVE-2015-1220 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVE-2015-1220

CVE-2015-1221 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-1221

CVE-2015-1222 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-1222

CVE-2015-1224 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-17
CVE-2015-1224

CVE-2015-1227 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-399
CVE-2015-1227

CVE-2015-1228 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-399
CVE-2015-1228

CVE-2015-1229 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-19
CVE-2015-1229

CVE-2015-1231 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-1231

CVE-2015-2238 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-2238

Обновление Риск: Высокий

ALTX ID 67054	**Обновление USN-2536-1 -- уязвимости libXfont**

Описание

Ilja van Sprundel, Alan Coopersmith, and William Robinet discovered that libXfont incorrectly handled malformed bdf fonts. A local attacker could use this issue to cause libXfont to crash, or possibly execute arbitrary code in order to gain privileges.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7632
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7632

USN-2536-1 (VENDOR)
USN-2536-1

CVE-2015-1802 (CVE)
CVSS: Базовая оценка 8.5 (AV:N/AC:M/Au:S/C:C/I:C/A:C)
CWE: CWE-119
CVE-2015-1802

CVE-2015-1803 (CVE)
CVSS: Базовая оценка 8.5 (AV:N/AC:M/Au:S/C:C/I:C/A:C)
CVE-2015-1803

CVE-2015-1804 (CVE)
CVSS: Базовая оценка 8.5 (AV:N/AC:M/Au:S/C:C/I:C/A:C)
CWE: CWE-189
CVE-2015-1804

Обновление Риск: Высокий

ALTX ID 67259	**Обновление USN-2538-1 -- уязвимости Firefox**

Описание

A flaw was discovered in the implementation of typed array bounds checking in the Javascript just-in-time compilation. If a user were tricked in to opening a specially crafted website, an attacked could exploit this to execute arbitrary code with the privileges of the user invoking Firefox.

Mariusz Mlynski discovered a flaw in the processing of SVG format content navigation. If a user were tricked in to opening a specially crafted website, an attacker could exploit this to run arbitrary script in a privileged context.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7651
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7651

USN-2538-1 (VENDOR)
USN-2538-1

CVE-2015-0817 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-17
CVE-2015-0817

CVE-2015-0818 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-264
CVE-2015-0818

Обновление Риск: Высокий

ALTX ID 67050	**Обновление USN-2532-1 -- уязвимость cups-filters**

Описание

It was discovered that cups-browsed incorrectly filtered remote printer names and strings. A remote attacker could use this issue to possibly execute arbitrary commands.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7628

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7628

USN-2532-1 (VENDOR)

USN-2532-1

CVE-2015-2265 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-77
CVE-2015-2265

Обновление Риск: Высокий

ALTX ID 66588	**Обновление USN-2506-1 -- уязвимости Thunderbird**

Описание

Armin Razmdjou discovered that contents of locally readable files could be made available via manipulation of form autocomplete in some circumstances. If a user were tricked in to opening a specially crafted message with scripting enabled, an attacker could potentially exploit this to obtain sensitive information.

Abhishek Arya discovered an out-of-bounds read and write when rendering SVG content in some circumstances. If a user were tricked in to opening a specially crafted message with scripting enabled, an attacker could potentially exploit this to obtain sensitive information.

Paul Bandha discovered a use-after-free in IndexedDB. If a user were tricked in to opening a specially crafted message with scripting enabled, an attacker could potentially exploit this to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Thunderbird.

Carsten Book, Christoph Diehl, Gary Kwong, Jan de Mooij, Liz Henry, Byron

Campen, Tom Schuster, and Ryan VanderMeulen discovered multiple memory safety issues in Thunderbird. If a user were tricked in to opening a specially crafted message with scripting enabled, an attacker could potentially exploit these to cause a denial of service via application crash, or execute arbitrary code with the privileges of the user invoking Thunderbird.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7520
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7520

USN-2506-1 (VENDOR)
USN-2506-1

CVE-2015-0822 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE: CWE-200
CVE-2015-0822

CVE-2015-0827 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)
CWE: CWE-119
CVE-2015-0827

CVE-2015-0831 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVE-2015-0831

CVE-2015-0836 (CVE)
CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVE-2015-0836

Обновление Риск: Высокий

ALTX ID 66589	**Обновление USN-2516-3 -- регрессия Linux kernel vulnerabilities**

Описание

A flaw was discovered in the Kernel Virtual Machine's (KVM) emulation of the SYSTENTER instruction when the guest OS does not initialize the SYSENTER MSRs. A guest OS user could exploit this flaw to cause a denial of service of the guest OS (crash) or potentially gain privileges on the guest OS.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7521
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7521

USN-2516-3 (VENDOR)
USN-2516-3

CVE-2015-0239 (CVE)
CVSS: Базовая оценка 4.7 (AV:L/AC:H/Au:N/C:N/I:P/A:C)
CWE: CWE-362
CVE-2015-0239

CVE-2014-8133 (CVE)
CVSS: Базовая оценка 2.1 (AV:L/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-264
CVE-2014-8133

CVE-2014-8160 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-254
CVE-2014-8160

CVE-2014-8559 (CVE)
CVSS: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)
CWE: CWE-399
CVE-2014-8559

CVE-2014-8989 (CVE)
CVSS: Базовая оценка 4.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-264
CVE-2014-8989

CVE-2014-9419 (CVE)
CVSS: Базовая оценка 2.1 (AV:L/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-200
CVE-2014-9419

CVE-2014-9420 (CVE)
CVSS: Базовая оценка 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)
CWE: CWE-399
CVE-2014-9420

CVE-2014-9428 (CVE)
CVSS: Базовая оценка 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
CWE: CWE-399
CVE-2014-9428

CVE-2014-9529 (CVE)
CVSS: Базовая оценка 7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
CWE: CWE-362
CVE-2014-9529

CVE-2014-9584 (CVE)
CVSS: Базовая оценка 2.1 (AV:L/AC:L/Au:N/C:P/I:N/A:N)
CWE: CWE-20
CVE-2014-9584

CVE-2014-9585 (CVE)
CVSS: Базовая оценка 2.1 (AV:L/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-264
CVE-2014-9585

CVE-2014-9683 (CVE)
CVSS: Базовая оценка 3.6 (AV:L/AC:L/Au:N/C:N/I:P/A:P)
CWE: CWE-189
CVE-2014-9683

Обновление	Риск: Средний
ALTX ID 69759	**Обновление USN-2571-1 -- уязвимость Firefox**
Описание	

Robert Kaiser discovered a use-after-free during plugin initialization in some circumstances. If a user were tricked in to opening a specially

crafted website, an attacker could potentially exploit this to cause a denial of service via application crash or execute arbitrary code with the privileges of the user invoking Firefox.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7825

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7825

USN-2571-1 (VENDOR)

USN-2571-1

CVE-2015-2706 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CWE: CWE-362
CVE-2015-2706

Обновление Риск: Средний

ALTX ID 69935	**Обновление USN-2581-1 -- уязвимость NetworkManager**

Описание

Tavis Ormandy discovered that NetworkManager incorrectly filtered paths when requested to read modem device contexts. A local attacker could possibly use this issue to bypass privileges and manipulate modem device configuration or read arbitrary files.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7837

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7837

USN-2581-1 (VENDOR)

USN-2581-1

CVE-2015-1322 (CVE)

CVSS: Базовая оценка 4.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-22
CVE-2015-1322

Обновление Риск: Средний

ALTX ID 66786	**Обновление USN-2528-1 -- уязвимость Linux kernel**

Описание

It was discovered that the Linux kernel's Infiniband subsystem did not properly sanitize its input parameters while registering memory regions from userspace. A local user could exploit this flaw to cause a denial of service (system crash) or to potentially gain administrative privileges.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7594

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7594

USN-2528-1 (VENDOR)

USN-2528-1

CVE-2014-8159 (CVE)

CVSS: Базовая оценка 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)
CWE: CWE-264
CVE-2014-8159

Обновление Риск: Средний

ALTX ID 70983	**Обновление USN-2593-1 -- уязвимость Dnsmasq**

Описание

Nick Sampanis discovered that Dnsmasq incorrectly handled certain malformed DNS requests. A remote attacker could use this issue to cause Dnsmasq to crash, resulting in a denial of service, or possibly obtain sensitive information.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7874

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7874

USN-2593-1 (VENDOR)

USN-2593-1

CVE-2015-3294 (CVE)

CVSS: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P)
CWE: CWE-19
CVE-2015-3294

Обновление Риск: Средний

ALTX ID 70984	**Обновление USN-2595-1 -- уязвимость ppp**

Описание

It was discovered that ppp incorrectly handled large PIDs. When pppd is used with a RADIUS server, a remote attacker could use this issue to cause it to crash, resulting in a denial of service.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7875

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7875

USN-2595-1 (VENDOR)

USN-2595-1

CVE-2015-3310 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)
CWE: CWE-119
CVE-2015-3310

Обновление Риск: Средний

ALTX ID 67491	**Обновление USN-2557-1 -- уязвимость Firefox**

Описание

Muneaki Nishimura discovered a flaw in Mozilla's HTTP Alternative Services implementation which meant SSL certificate verification could be bypassed in some circumstances. A remote attacker could potentially exploit this to conduct a man in the middle attack.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7753

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7753

USN-2557-1 (VENDOR)

USN-2557-1

CVE-2015-0799 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-20
CVE-2015-0799

Обновление Риск: Средний

ALTX ID 69758	**Обновление USN-2576-1 -- уязвимость usb-creator**

Описание

Tavis Ormandy discovered that usb-creator was missing an authentication check. A local attacker could use this issue to gain elevated privileges.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7824

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7824

USN-2576-1 (VENDOR)

USN-2576-1

Обновление Риск: Средний

ALTX ID 67446	**Обновление USN-2553-2 -- регрессия LibTIFF**

Описание

William Robinet discovered that LibTIFF incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7730
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7730

USN-2553-2 (VENDOR)
USN-2553-2

CVE-2014-8127 (CVE)
CVE-2014-8127

CVE-2014-8128 (CVE)
CVE-2014-8128

CVE-2014-8129 (CVE)
CVE-2014-8129

CVE-2014-8130 (CVE)
CVE-2014-8130

CVE-2014-9330 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-189
CVE-2014-9330

CVE-2014-9655 (CVE)
CVE-2014-9655

Обновление Риск: Средний

ALTX ID 67319

Обновление USN-2549-1 -- уязвимости libarchive

Описание

It was discovered that the libarchive bsdcpio utility extracted absolute paths by default without using the --insecure flag, contrary to expectations. If a user or automated system were tricked into extracting cpio archives containing absolute paths, a remote attacker may be able to write to arbitrary files.

Fabian Yamaguchi discovered that libarchive incorrectly handled certain type conversions. A remote attacker could possibly use this issue to cause libarchive to crash, resulting in a denial of service. This issue only affected Ubuntu 12.04 LTS.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7684
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7684

USN-2549-1 (VENDOR)
USN-2549-1

CVE-2015-2304 (CVE)

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

CWE: CWE-22

CVE-2015-2304

CVE-2013-0211 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-189

CVE-2013-0211

Обновление Риск: Средний

ALTX ID 67443	**Обновление USN-2555-1 -- уязвимости Libgcrypt**

Описание

Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer discovered that Libgcrypt was susceptible to an attack via physical side channels. A local attacker could use this attack to possibly recover private keys.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7727

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7727

USN-2555-1 (VENDOR)

USN-2555-1

CVE-2014-3591 (CVE)

CVE-2014-3591

CVE-2015-0837 (CVE)

CVE-2015-0837

Обновление Риск: Средний

ALTX ID 67317	**Обновление USN-2540-1 -- уязвимости GnuTLS**

Описание

It was discovered that GnuTLS did not perform date and time checks on CA certificates, contrary to expectations. This issue only affected Ubuntu 10.04 LTS.

Nikos Mavrogiannopoulos discovered that GnuTLS incorrectly verified that signature algorithms matched. A remote attacker could possibly use this issue to downgrade to a disallowed algorithm. This issue only affected Ubuntu 10.04 LTS, Ubuntu 12.04 LTS and Ubuntu 14.04 LTS.

It was discovered that GnuTLS incorrectly verified certificate algorithms. A remote attacker could possibly use this issue to downgrade to a disallowed algorithm.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7682
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7682

USN-2540-1 (VENDOR)
USN-2540-1

CVE-2014-8155 (CVE)
CVE-2014-8155

CVE-2015-0282 (CVE)
CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
CWE: CWE-310
CVE-2015-0282

CVE-2015-0294 (CVE)
CVE-2015-0294

Обновление Риск: Средний

ALTX ID 68482	**Обновление USN-2566-1 -- уязвимость dpkg**

Описание

Jann Horn discovered that dpkg incorrectly validated signatures when extracting local source packages. If a user or an automated system were tricked into unpacking a specially crafted source package, a remote attacker could bypass signature verification checks.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7775
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7775

USN-2566-1 (VENDOR)
USN-2566-1

CVE-2015-0840 (CVE)
CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)
CWE: CWE-284
CVE-2015-0840

Обновление Риск: Средний

ALTX ID 67441	**Обновление USN-2553-1 -- уязвимости LibTIFF**

Описание

William Robinet discovered that LibTIFF incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7725

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7725

USN-2553-1 (VENDOR)

USN-2553-1

CVE-2014-8127 (CVE)

CVE-2014-8127

CVE-2014-8128 (CVE)

CVE-2014-8128

CVE-2014-8129 (CVE)

CVE-2014-8129

CVE-2014-8130 (CVE)

CVE-2014-8130

CVE-2014-9330 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
CWE: CWE-189
CVE-2014-9330

CVE-2014-9655 (CVE)

CVE-2014-9655

Обновление Риск: Средний

ALTX ID 69756	**Обновление USN-2577-1 -- уязвимость wpa_supplicant**

Описание

It was discovered that wpa_supplicant incorrectly handled SSID information when creating or updating P2P peer entries. A remote attacker could use this issue to cause wpa_supplicant to crash, resulting in a denial of service, expose memory contents, or possibly execute arbitrary code.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7822

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7822

USN-2577-1 (VENDOR)

USN-2577-1

CVE-2015-1863 (CVE)

CVSS: Базовая оценка 5.8 (AV:A/AC:L/Au:N/C:P/I:P/A:P)
CWE: CWE-119
CVE-2015-1863

Обновление Риск: Средний

ALTX ID 67052	**Обновление USN-2531-1 -- уязвимость Requests**

Описание

Matthew Daley discovered that Requests incorrectly handled cookies without host values when being redirected. A remote attacker could possibly use this issue to perform session fixation or cookie stealing attacks.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7630
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7630

USN-2531-1 (VENDOR)
USN-2531-1

CVE-2015-2296 (CVE)
CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVE-2015-2296

Обновление Риск: Низкий

ALTX ID 67492	**Обновление USN-2559-1 -- уязвимость Libtasn1**

Описание

Hanno discovered that Libtasn1 incorrectly handled certain ASN.1 data. A remote attacker could possibly exploit this with specially crafted ASN.1 data and cause applications using Libtasn1 to crash, resulting in a denial of service, or possibly execute arbitrary code.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7754
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7754

USN-2559-1 (VENDOR)
USN-2559-1

CVE-2015-2806 (CVE)
CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
CWE: CWE-119
CVE-2015-2806

Обновление Риск: Низкий

ALTX ID 70998	**Обновление USN-2605-1 -- уязвимости ICU**

Описание

Pedro Ribeiro discovered that ICU incorrectly handled certain memory operations when processing data. If an application using ICU processed crafted data, an attacker could cause it to crash or potentially execute arbitrary code with the privileges of the user invoking the program.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7889
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7889

USN-2605-1 (VENDOR)
USN-2605-1
CVE-2014-8146 (CVE)
CVE-2014-8146
CVE-2014-8147 (CVE)
CVE-2014-8147

Обновление Риск: Низкий

ALTX ID 69551	**Обновление USN-2569-2 -- уязвимость Apport**

Описание

USN-2569-1 fixed a vulnerability in Apport. Tavis Ormandy discovered that the fixed packages were still vulnerable to a privilege escalation attack. This update completely disables crash report handling for containers until a more complete solution is available.

Original advisory details:

StГ©phane Graber and Tavis Ormandy independently discovered that Apport incorrectly handled the crash reporting feature. A local attacker could use this issue to gain elevated privileges.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7797
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7797
USN-2569-2 (VENDOR)
USN-2569-2

Обновление Риск: Низкий

ALTX ID 67444	**Обновление USN-2554-1 -- уязвимости GnuPG**

Описание

Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer discovered that GnuPG was susceptible to an attack via physical side channels. A local attacker could use this attack to possibly recover private keys.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.nix:def:7728
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.nix:def:7728
USN-2554-1 (VENDOR)
USN-2554-1
CVE-2014-3591 (CVE)
CVE-2014-3591

CVE-2015-0837 (CVE)

CVE-2015-0837

CVE-2015-1606 (CVE)

CVE-2015-1606

CVE-2015-1607 (CVE)

CVE-2015-1607

CVE-2014-5270 (CVE)

CVSS: Базовая оценка 2.1 (AV:L/AC:L/Au:N/C:P/I:N/A:N)

CWE: CWE-200

CVE-2014-5270

Конец отчета. RedCheck 1.4.1.1.
RedCheckID: 6DF9800A-476F-43D7-B922-36DDF894130F.