2017-DEC-21
FSL version 7.5.982

MCAFEE FOUNDSTONE FSL UPDATE

To better protect your environment McAfee has created this FSL check update for the Foundstone Product Suite. The following is a detailed summary of the new and updated checks included with this release.

NEW CHECKS

22788 - (HPESBHF03746) HPE Intelligent Management Center Multiple Vulnerabilities

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-5820, CVE-2017-5821, CVE-2017-5822, CVE-2017-5823

Description

Multiple remote code execution vulnerabilities are present in some versions of HPE Intelligent Management Center.

Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

Multiple remote code execution vulnerabilities are present in some versions of HPE Intelligent Management Center. The flaws lie in several components. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22804 - (HPESBHF03787) HPE Intelligent Management Center Multiple Vulnerabilities

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-8962, CVE-2017-8963, CVE-2017-8964, CVE-2017-8965, CVE-2017-8966, CVE-2017-8967

Description

Multiple vulnerabilities are present in some versions of HPE Intelligent Management Center.

Observation

HPE Intelligent Management Center (iMC) is an enterprise-class network management platform.

Multiple vulnerabilities are present in some versions of HPE Intelligent Management Center. The flaws lie in several components. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22864 - Google Chrome Multiple Vulnerabilities Prior To 63.0.3239.84

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-15407, CVE-2017-15408, CVE-2017-15409, CVE-2017-15410, CVE-2017-15411, CVE-2017-15412, CVE-2017-15413, CVE-2017-15415, CVE-2017-15416, CVE-2017-15417, CVE-2017-15418, CVE-2017-15419, CVE-2017-15420, CVE-2017-15422, CVE-2017-15423, CVE-2017-15424, CVE-2017-15425, CVE-2017-15426, CVE-2017-15427

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to conduct spoofing attacks, cause a buffer overflow, or execute arbitrary code affecting integrity, confidentiality or availability.

22865 - Google Chrome Multiple Vulnerabilities Prior To 63.0.3239.84

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-15407, CVE-2017-15408, CVE-2017-15409, CVE-2017-15410, CVE-2017-15411, CVE-2017-15412, CVE-2017-15413, CVE-2017-15415, CVE-2017-15416, CVE-2017-15417, CVE-2017-15418, CVE-2017-15419, CVE-2017-15420, CVE-2017-15422, CVE-2017-15423, CVE-2017-15424, CVE-2017-15425, CVE-2017-15426, CVE-2017-15427

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular web browser.

Multiple vulnerabilities are present in some versions of Google Chrome. The flaws lie in multiple components. Successful exploitation could allow an attacker to conduct spoofing attacks, cause a buffer overflow, or execute arbitrary code affecting integrity, confidentiality or availability.

132421 - Oracle VM OVMSA-2017-0174 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-10044, CVE-2016-10200, CVE-2016-10318, CVE-2016-1575, CVE-2016-1576, CVE-2016-6213, CVE-2016-9191, CVE-2016-9604, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-1000251, CVE-2017-1000363, CVE-2017-1000364, CVE-2017-1000365, CVE-2017-1000380, CVE-2017-1000405, CVE-2017-10661, CVE-2017-11176, CVE-2017-11473, CVE-2017-12134, CVE-2017-12154, CVE-2017-12190, CVE-2017-12192, CVE-2017-14106, CVE-2017-14489, CVE-2017-15649, CVE-2017-16527, CVE-2017-16650, CVE-2017-2618, CVE-2017-2671, CVE-2017-7477, CVE-2017-7482, CVE-2017-7533, CVE-2017-7541, CVE-2017-7542, CVE-2017-7618, CVE-2017-7645, CVE-2017-7889, CVE-2017-8797, CVE-2017-8831, CVE-2017-8890, CVE-2017-9059, CVE-2017-9074, CVE-2017-9075, CVE-2017-9077, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0174

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/oraclevm-errata/2017-December/000805.html

OVM3.4
x86_64
kernel-uek-4.1.12-112.14.1.el6uek
kernel-uek-firmware-4.1.12-112.14.1.el6uek

163514 - Oracle Enterprise Linux ELSA-2017-3659 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-10044, CVE-2016-10200, CVE-2016-10318, CVE-2016-1575, CVE-2016-1576, CVE-2016-6213, CVE-2016-9191, CVE-2016-9604, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-1000251, CVE-2017-1000363, CVE-2017-1000364, CVE-2017-1000365, CVE-2017-1000380, CVE-2017-1000405, CVE-2017-10661, CVE-2017-11176, CVE-2017-11473, CVE-2017-12134, CVE-2017-12154, CVE-2017-12190, CVE-2017-12192, CVE-2017-14106, CVE-2017-14489, CVE-2017-15649, CVE-2017-16527, CVE-2017-16650, CVE-2017-2618, CVE-2017-2671, CVE-2017-7477, CVE-2017-7482, CVE-2017-7533, CVE-2017-7541, CVE-2017-7542, CVE-2017-7618, CVE-2017-7645, CVE-2017-7889, CVE-2017-8797, CVE-2017-8831, CVE-2017-8890, CVE-2017-9059, CVE-2017-9074, CVE-2017-9075, CVE-2017-9077, CVE-2017-9242

Description

The scan detected that the host is missing the following update:
ELSA-2017-3659

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/el-errata/2017-December/007418.html
http://oss.oracle.com/pipermail/el-errata/2017-December/007417.html

OEL7
x86_64
kernel-uek-debug-devel-4.1.12-112.14.1.el7uek
kernel-uek-devel-4.1.12-112.14.1.el7uek
kernel-uek-firmware-4.1.12-112.14.1.el7uek
kernel-uek-doc-4.1.12-112.14.1.el7uek
kernel-uek-4.1.12-112.14.1.el7uek
kernel-uek-debug-4.1.12-112.14.1.el7uek

OEL6
x86_64
kernel-uek-doc-4.1.12-112.14.1.el6uek
kernel-uek-4.1.12-112.14.1.el6uek
kernel-uek-devel-4.1.12-112.14.1.el6uek
kernel-uek-debug-4.1.12-112.14.1.el6uek
kernel-uek-firmware-4.1.12-112.14.1.el6uek
kernel-uek-debug-devel-4.1.12-112.14.1.el6uek

22810 - Geovap Reliance SCADA Cross-Site Scripting Vulnerability

Category: Windows Host Assessment -> SCADA
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-16721

Description

A cross-site scripting vulnerability is present in some versions of Geovap Reliance SCADA.

Observation

Geovap Reliance SCADA Software is a HMI/SCADA software used to create robust HMI screens to control machine, process.

A cross-site scripting vulnerability is present in some versions of Geovap Reliance SCADA. The flaw is due to improper validating URL requests. Successful exploitation could allow a remote attacker to read/write access.

141807 - Red Hat Enterprise Linux RHSA-2017-3485 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-0898, CVE-2017-0899, CVE-2017-0900, CVE-2017-0901, CVE-2017-0902, CVE-2017-0903, CVE-2017-10784, CVE-2017-14064

Description

The scan detected that the host is missing the following update:
RHSA-2017-3485

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00037.html

RHEL7S
x86_64
rh-ruby24-rubygem-json-2.0.4-86.el7
rh-ruby24-rubygem-net-telnet-0.1.1-86.el7
rh-ruby24-rubygem-did_you_mean-1.1.0-86.el7
rh-ruby24-ruby-2.4.2-86.el7
rh-ruby24-rubygem-io-console-0.4.6-86.el7
rh-ruby24-rubygem-psych-2.2.2-86.el7
rh-ruby24-rubygem-openssl-2.0.5-86.el7
rh-ruby24-ruby-libs-2.4.2-86.el7
rh-ruby24-ruby-devel-2.4.2-86.el7
rh-ruby24-ruby-debuginfo-2.4.2-86.el7
rh-ruby24-rubygem-bigdecimal-1.3.0-86.el7

noarch
rh-ruby24-rubygem-power_assert-0.4.1-86.el7
rh-ruby24-rubygems-2.6.14-86.el7
rh-ruby24-rubygem-test-unit-3.2.3-86.el7
rh-ruby24-rubygem-xmlrpc-0.2.1-86.el7
rh-ruby24-rubygems-devel-2.6.14-86.el7
rh-ruby24-rubygem-rdoc-5.0.0-86.el7
rh-ruby24-rubygem-minitest-5.10.1-86.el7
rh-ruby24-ruby-irb-2.4.2-86.el7
rh-ruby24-ruby-doc-2.4.2-86.el7
rh-ruby24-rubygem-rake-12.0.0-86.el7

RHEL6S
x86_64
rh-ruby24-rubygem-json-2.0.4-86.el6
rh-ruby24-rubygem-psych-2.2.2-86.el6
rh-ruby24-ruby-2.4.2-86.el6
rh-ruby24-rubygem-io-console-0.4.6-86.el6
rh-ruby24-rubygem-net-telnet-0.1.1-86.el6
rh-ruby24-ruby-libs-2.4.2-86.el6
rh-ruby24-rubygem-bigdecimal-1.3.0-86.el6
rh-ruby24-ruby-debuginfo-2.4.2-86.el6
rh-ruby24-ruby-devel-2.4.2-86.el6
rh-ruby24-rubygem-did_you_mean-1.1.0-86.el6
rh-ruby24-rubygem-openssl-2.0.5-86.el6

noarch

rh-ruby24-rubygem-power_assert-0.4.1-86.el6
rh-ruby24-rubygem-rake-12.0.0-86.el6
rh-ruby24-rubygems-devel-2.6.14-86.el6
rh-ruby24-rubygem-minitest-5.10.1-86.el6
rh-ruby24-rubygem-test-unit-3.2.3-86.el6
rh-ruby24-rubygems-2.6.14-86.el6
rh-ruby24-ruby-doc-2.4.2-86.el6
rh-ruby24-ruby-irb-2.4.2-86.el6
rh-ruby24-rubygem-rdoc-5.0.0-86.el6
rh-ruby24-rubygem-xmlrpc-0.2.1-86.el6

RHEL6WS
x86_64
rh-ruby24-rubygem-json-2.0.4-86.el6
rh-ruby24-rubygem-psych-2.2.2-86.el6
rh-ruby24-ruby-2.4.2-86.el6
rh-ruby24-rubygem-io-console-0.4.6-86.el6
rh-ruby24-rubygem-net-telnet-0.1.1-86.el6
rh-ruby24-ruby-libs-2.4.2-86.el6
rh-ruby24-rubygem-bigdecimal-1.3.0-86.el6
rh-ruby24-ruby-debuginfo-2.4.2-86.el6
rh-ruby24-ruby-devel-2.4.2-86.el6
rh-ruby24-rubygem-did_you_mean-1.1.0-86.el6
rh-ruby24-rubygem-openssl-2.0.5-86.el6

noarch
rh-ruby24-rubygem-power_assert-0.4.1-86.el6
rh-ruby24-rubygem-rake-12.0.0-86.el6
rh-ruby24-rubygems-devel-2.6.14-86.el6
rh-ruby24-rubygem-minitest-5.10.1-86.el6
rh-ruby24-rubygem-test-unit-3.2.3-86.el6
rh-ruby24-rubygems-2.6.14-86.el6
rh-ruby24-ruby-doc-2.4.2-86.el6
rh-ruby24-ruby-irb-2.4.2-86.el6
rh-ruby24-rubygem-rdoc-5.0.0-86.el6
rh-ruby24-rubygem-xmlrpc-0.2.1-86.el6

RHEL6_7S
x86_64
rh-ruby24-rubygem-json-2.0.4-86.el6
rh-ruby24-rubygem-psych-2.2.2-86.el6
rh-ruby24-ruby-2.4.2-86.el6
rh-ruby24-rubygem-io-console-0.4.6-86.el6
rh-ruby24-rubygem-net-telnet-0.1.1-86.el6
rh-ruby24-ruby-libs-2.4.2-86.el6
rh-ruby24-rubygem-bigdecimal-1.3.0-86.el6
rh-ruby24-ruby-debuginfo-2.4.2-86.el6
rh-ruby24-ruby-devel-2.4.2-86.el6
rh-ruby24-rubygem-did_you_mean-1.1.0-86.el6
rh-ruby24-rubygem-openssl-2.0.5-86.el6

noarch
rh-ruby24-rubygem-power_assert-0.4.1-86.el6
rh-ruby24-rubygem-rake-12.0.0-86.el6
rh-ruby24-rubygems-devel-2.6.14-86.el6
rh-ruby24-rubygem-minitest-5.10.1-86.el6
rh-ruby24-rubygem-test-unit-3.2.3-86.el6
rh-ruby24-rubygems-2.6.14-86.el6
rh-ruby24-ruby-doc-2.4.2-86.el6
rh-ruby24-ruby-irb-2.4.2-86.el6

rh-ruby24-rubygem-rdoc-5.0.0-86.el6
rh-ruby24-rubygem-xmlrpc-0.2.1-86.el6

RHEL7_3S
x86_64
rh-ruby24-rubygem-json-2.0.4-86.el7
rh-ruby24-rubygem-net-telnet-0.1.1-86.el7
rh-ruby24-rubygem-did_you_mean-1.1.0-86.el7
rh-ruby24-ruby-2.4.2-86.el7
rh-ruby24-rubygem-io-console-0.4.6-86.el7
rh-ruby24-rubygem-psych-2.2.2-86.el7
rh-ruby24-rubygem-openssl-2.0.5-86.el7
rh-ruby24-ruby-libs-2.4.2-86.el7
rh-ruby24-ruby-devel-2.4.2-86.el7
rh-ruby24-ruby-debuginfo-2.4.2-86.el7
rh-ruby24-rubygem-bigdecimal-1.3.0-86.el7

noarch
rh-ruby24-rubygem-power_assert-0.4.1-86.el7
rh-ruby24-rubygems-2.6.14-86.el7
rh-ruby24-rubygem-test-unit-3.2.3-86.el7
rh-ruby24-rubygem-xmlrpc-0.2.1-86.el7
rh-ruby24-rubygems-devel-2.6.14-86.el7
rh-ruby24-rubygem-rdoc-5.0.0-86.el7
rh-ruby24-rubygem-minitest-5.10.1-86.el7
rh-ruby24-ruby-irb-2.4.2-86.el7
rh-ruby24-ruby-doc-2.4.2-86.el7
rh-ruby24-rubygem-rake-12.0.0-86.el7

RHEL7WS
x86_64
rh-ruby24-rubygem-json-2.0.4-86.el7
rh-ruby24-rubygem-net-telnet-0.1.1-86.el7
rh-ruby24-rubygem-did_you_mean-1.1.0-86.el7
rh-ruby24-ruby-2.4.2-86.el7
rh-ruby24-rubygem-io-console-0.4.6-86.el7
rh-ruby24-rubygem-psych-2.2.2-86.el7
rh-ruby24-rubygem-openssl-2.0.5-86.el7
rh-ruby24-ruby-libs-2.4.2-86.el7
rh-ruby24-ruby-devel-2.4.2-86.el7
rh-ruby24-ruby-debuginfo-2.4.2-86.el7
rh-ruby24-rubygem-bigdecimal-1.3.0-86.el7

noarch
rh-ruby24-rubygem-power_assert-0.4.1-86.el7
rh-ruby24-rubygems-2.6.14-86.el7
rh-ruby24-rubygem-test-unit-3.2.3-86.el7
rh-ruby24-rubygem-xmlrpc-0.2.1-86.el7
rh-ruby24-rubygems-devel-2.6.14-86.el7
rh-ruby24-rubygem-rdoc-5.0.0-86.el7
rh-ruby24-rubygem-minitest-5.10.1-86.el7
rh-ruby24-ruby-irb-2.4.2-86.el7
rh-ruby24-ruby-doc-2.4.2-86.el7
rh-ruby24-rubygem-rake-12.0.0-86.el7

22849 - Cisco NX-OS Software Patch Signature Bypass Vulnerability (cisco-sa-20171129-nxos)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-12331

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS is a network operating system .

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to insufficient NX-OS signature verification for software patches. Successful exploitation could allow a remote attacker to load a software patch bypassing such security mechanism.

22852 - PHOENIX CONTACT COMSERVER Cross-Site Scripting Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: High

CVE: CVE-2017-16723

Description

A vulnerability is present in some versions of PHOENIX CONTACT FL COMSERVER.

Observation

PHOENIX CONTACT FL COMSERVER is a serial device for converting a serial RS-232/422/485 interface to Ethernet.

A vulnerability is present in some versions of PHOENIX CONTACT FL COMSERVER. The flaw is due to improper handling of user input. Successful exploitation could allow an attacker to remotely change configuration variables on the device.

22803 - Cisco Nexus Series Switches CLI Command Injection Vulnerability (cisco-sa-20171129-nss)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-12330

Description

A command-injection vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A command injection vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to improper input validation of CLI command arguments. Successful exploitation could allow an attacker to execute arbitrary commands.

22857 - (SB10211) McAfee Web Gateway Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-2853, CVE-2017-16525, CVE-2017-16531, CVE-2017-16533, CVE-2017-16535, CVE-2017-3735, CVE-2017-3736

Description

Multiple vulnerabilities are present in some versions of McAfee Web Gateway.

Observation

McAfee Web Gateway is a web based security control system designed to prevent web application attacks.

Multiple vulnerabilities are present in some versions of McAfee Web Gateway. The flaws lie in several components. Successful exploitation could allow an attacker to cause a denial of service condition or have other unspecified impact on the target system.

22876 - (HT208328) Apple iCloud Vulnerabilities Prior To 7.2

Category: Windows Host Assessment -> Miscellaneous
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-13856, CVE-2017-13864, CVE-2017-13866, CVE-2017-13870, CVE-2017-7156, CVE-2017-7157

Description

Multiple vulnerabilities are present in some versions of Apple iCloud.

Observation

Apple iCloud is a manager for the Apple's cloud-based storage service.

Multiple vulnerabilities are present in some versions of Apple iCloud. The flaw lies in multiple components.Successful exploitation could allow an attacker to execute remote arbitrary code or bypass security measures.

130976 - Debian Linux 8.0, 9.0 DSA-4068-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-16548, CVE-2017-17433, CVE-2017-17434

Description

The scan detected that the host is missing the following update:
DSA-4068-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2017/dsa-4068

Debian 8.0
all
rsync_3.1.1-3+deb8u1

Debian 9.0
all
rsync_3.1.2-1+deb9u1

132418 - Oracle VM OVMSA-2017-0178 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-15592, CVE-2017-17044, CVE-2017-17045

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0178

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/oraclevm-errata/2017-December/000810.html

OVM3.2
x86_64
xen-devel-4.1.3-25.el5.223.99
xen-tools-4.1.3-25.el5.223.99
xen-4.1.3-25.el5.223.99

132419 - Oracle VM OVMSA-2017-0176 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-15592, CVE-2017-15595, CVE-2017-17044, CVE-2017-17045

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0176

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/oraclevm-errata/2017-December/000808.html

OVM3.4
x86_64
xen-tools-4.4.4-155.0.7.el6
xen-4.4.4-155.0.7.el6

132420 - Oracle VM OVMSA-2017-0177 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-15592, CVE-2017-17044, CVE-2017-17045

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0177

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://oss.oracle.com/pipermail/oraclevm-errata/2017-December/000809.html

OVM3.3
x86_64
xen-4.3.0-55.el6.186.63
xen-tools-4.3.0-55.el6.186.63

141808 - Red Hat Enterprise Linux RHSA-2017-3479 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-15429

Description

The scan detected that the host is missing the following update:
RHSA-2017-3479

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00034.html

RHEL6D
x86_64
chromium-browser-debuginfo-63.0.3239.108-1.el6_9
chromium-browser-63.0.3239.108-1.el6_9

i386
chromium-browser-debuginfo-63.0.3239.108-1.el6_9
chromium-browser-63.0.3239.108-1.el6_9

RHEL6S
x86_64
chromium-browser-debuginfo-63.0.3239.108-1.el6_9
chromium-browser-63.0.3239.108-1.el6_9

i386
chromium-browser-debuginfo-63.0.3239.108-1.el6_9
chromium-browser-63.0.3239.108-1.el6_9

RHEL6WS
x86_64
chromium-browser-debuginfo-63.0.3239.108-1.el6_9
chromium-browser-63.0.3239.108-1.el6_9

i386
chromium-browser-debuginfo-63.0.3239.108-1.el6_9
chromium-browser-63.0.3239.108-1.el6_9

141809 - Red Hat Enterprise Linux RHSA-2017-3463 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-15041, CVE-2017-15042

Description

The scan detected that the host is missing the following update:
RHSA-2017-3463

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.redhat.com/archives/rhsa-announce/2017-December/msg00024.html

RHEL7S
noarch
go-toolset-7-golang-misc-1.8.5-1.el7
go-toolset-7-golang-docs-1.8.5-1.el7
go-toolset-7-golang-src-1.8.5-1.el7
go-toolset-7-golang-tests-1.8.5-1.el7

x86_64
go-toolset-7-build-1.8-10.el7
go-toolset-7-golang-1.8.5-1.el7
go-toolset-7-dockerfiles-1.8-10.el7
go-toolset-7-scldevel-1.8-10.el7
go-toolset-7-golang-bin-1.8.5-1.el7
go-toolset-7-golang-race-1.8.5-1.el7
go-toolset-7-runtime-1.8-10.el7
go-toolset-7-1.8-10.el7

RHEL7WS
x86_64
go-toolset-7-build-1.8-10.el7
go-toolset-7-golang-1.8.5-1.el7
go-toolset-7-dockerfiles-1.8-10.el7
go-toolset-7-scldevel-1.8-10.el7
go-toolset-7-golang-bin-1.8.5-1.el7
go-toolset-7-golang-race-1.8.5-1.el7
go-toolset-7-runtime-1.8-10.el7
go-toolset-7-1.8-10.el7

noarch
go-toolset-7-golang-misc-1.8.5-1.el7
go-toolset-7-golang-docs-1.8.5-1.el7
go-toolset-7-golang-src-1.8.5-1.el7
go-toolset-7-golang-tests-1.8.5-1.el7

146162 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3329-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-16642, CVE-2017-4025, CVE-2017-9228, CVE-2017-9229

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3329-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.opensuse.org/opensuse-updates/2017-12/msg00055.html

SuSE Linux 42.2
i586
php5-posix-5.5.14-77.15.1
php5-ldap-debuginfo-5.5.14-77.15.1
php5-xmlwriter-5.5.14-77.15.1

php5-intl-debuginfo-5.5.14-77.15.1
php5-gd-5.5.14-77.15.1
php5-xmlrpc-5.5.14-77.15.1
php5-iconv-5.5.14-77.15.1
php5-tokenizer-5.5.14-77.15.1
php5-ftp-debuginfo-5.5.14-77.15.1
php5-fastcgi-5.5.14-77.15.1
php5-dba-5.5.14-77.15.1
php5-sysvshm-debuginfo-5.5.14-77.15.1
php5-bcmath-5.5.14-77.15.1
php5-suhosin-5.5.14-77.15.1
php5-wddx-debuginfo-5.5.14-77.15.1
php5-calendar-5.5.14-77.15.1
php5-sysvshm-5.5.14-77.15.1
php5-zip-debuginfo-5.5.14-77.15.1
php5-devel-5.5.14-77.15.1
php5-sysvmsg-debuginfo-5.5.14-77.15.1
php5-ctype-debuginfo-5.5.14-77.15.1
php5-openssl-5.5.14-77.15.1
php5-pcntl-5.5.14-77.15.1
php5-mbstring-debuginfo-5.5.14-77.15.1
php5-pgsql-debuginfo-5.5.14-77.15.1
php5-pspell-debuginfo-5.5.14-77.15.1
php5-mbstring-5.5.14-77.15.1
php5-iconv-debuginfo-5.5.14-77.15.1
php5-curl-debuginfo-5.5.14-77.15.1
php5-ldap-5.5.14-77.15.1
apache2-mod_php5-debuginfo-5.5.14-77.15.1
php5-tidy-5.5.14-77.15.1
php5-phar-debuginfo-5.5.14-77.15.1
php5-openssl-debuginfo-5.5.14-77.15.1
php5-sockets-debuginfo-5.5.14-77.15.1
php5-fileinfo-5.5.14-77.15.1
php5-pdo-debuginfo-5.5.14-77.15.1
php5-imap-debuginfo-5.5.14-77.15.1
php5-exif-5.5.14-77.15.1
php5-sockets-5.5.14-77.15.1
php5-debugsource-5.5.14-77.15.1
php5-gd-debuginfo-5.5.14-77.15.1
php5-shmop-debuginfo-5.5.14-77.15.1
php5-enchant-debuginfo-5.5.14-77.15.1
php5-snmp-5.5.14-77.15.1
php5-imap-5.5.14-77.15.1
php5-xsl-debuginfo-5.5.14-77.15.1
php5-calendar-debuginfo-5.5.14-77.15.1
php5-shmop-5.5.14-77.15.1
php5-intl-5.5.14-77.15.1
php5-mysql-5.5.14-77.15.1
php5-gmp-5.5.14-77.15.1
php5-odbc-5.5.14-77.15.1
php5-bz2-5.5.14-77.15.1
php5-xmlreader-5.5.14-77.15.1
php5-posix-debuginfo-5.5.14-77.15.1
php5-mssql-5.5.14-77.15.1
php5-pgsql-5.5.14-77.15.1
php5-sysvmsg-5.5.14-77.15.1
php5-xmlreader-debuginfo-5.5.14-77.15.1
php5-json-5.5.14-77.15.1
php5-bz2-debuginfo-5.5.14-77.15.1
php5-zlib-5.5.14-77.15.1

php5-sysvsem-5.5.14-77.15.1
php5-sqlite-debuginfo-5.5.14-77.15.1
php5-sqlite-5.5.14-77.15.1
php5-readline-5.5.14-77.15.1
php5-ftp-5.5.14-77.15.1
php5-firebird-debuginfo-5.5.14-77.15.1
php5-dom-5.5.14-77.15.1
php5-ctype-5.5.14-77.15.1
php5-fpm-debuginfo-5.5.14-77.15.1
php5-gmp-debuginfo-5.5.14-77.15.1
php5-firebird-5.5.14-77.15.1
php5-soap-5.5.14-77.15.1
php5-xsl-5.5.14-77.15.1
php5-enchant-5.5.14-77.15.1
php5-debuginfo-5.5.14-77.15.1
php5-soap-debuginfo-5.5.14-77.15.1
php5-exif-debuginfo-5.5.14-77.15.1
php5-dom-debuginfo-5.5.14-77.15.1
php5-odbc-debuginfo-5.5.14-77.15.1
php5-5.5.14-77.15.1
php5-fileinfo-debuginfo-5.5.14-77.15.1
php5-bcmath-debuginfo-5.5.14-77.15.1
php5-json-debuginfo-5.5.14-77.15.1
php5-curl-5.5.14-77.15.1
php5-wddx-5.5.14-77.15.1
php5-opcache-debuginfo-5.5.14-77.15.1
php5-snmp-debuginfo-5.5.14-77.15.1
php5-sysvsem-debuginfo-5.5.14-77.15.1
php5-pcntl-debuginfo-5.5.14-77.15.1
php5-tidy-debuginfo-5.5.14-77.15.1
php5-suhosin-debuginfo-5.5.14-77.15.1
php5-fastcgi-debuginfo-5.5.14-77.15.1
php5-mssql-debuginfo-5.5.14-77.15.1
php5-mcrypt-debuginfo-5.5.14-77.15.1
php5-mysql-debuginfo-5.5.14-77.15.1
php5-pspell-5.5.14-77.15.1
php5-xmlrpc-debuginfo-5.5.14-77.15.1
apache2-mod_php5-5.5.14-77.15.1
php5-mcrypt-5.5.14-77.15.1
php5-tokenizer-debuginfo-5.5.14-77.15.1
php5-fpm-5.5.14-77.15.1
php5-phar-5.5.14-77.15.1
php5-gettext-debuginfo-5.5.14-77.15.1
php5-readline-debuginfo-5.5.14-77.15.1
php5-zip-5.5.14-77.15.1
php5-gettext-5.5.14-77.15.1
php5-opcache-5.5.14-77.15.1
php5-dba-debuginfo-5.5.14-77.15.1
php5-xmlwriter-debuginfo-5.5.14-77.15.1
php5-zlib-debuginfo-5.5.14-77.15.1
php5-pdo-5.5.14-77.15.1

noarch
php5-pear-5.5.14-77.15.1

x86_64
php5-posix-5.5.14-77.15.1
php5-ldap-debuginfo-5.5.14-77.15.1
php5-xmlwriter-5.5.14-77.15.1
php5-intl-debuginfo-5.5.14-77.15.1

php5-gd-5.5.14-77.15.1
php5-xmlrpc-5.5.14-77.15.1
php5-iconv-5.5.14-77.15.1
php5-tokenizer-5.5.14-77.15.1
php5-ftp-debuginfo-5.5.14-77.15.1
php5-fastcgi-5.5.14-77.15.1
php5-dba-5.5.14-77.15.1
php5-sysvshm-debuginfo-5.5.14-77.15.1
php5-bcmath-5.5.14-77.15.1
php5-suhosin-5.5.14-77.15.1
php5-wddx-debuginfo-5.5.14-77.15.1
php5-calendar-5.5.14-77.15.1
php5-sysvshm-5.5.14-77.15.1
php5-zip-debuginfo-5.5.14-77.15.1
php5-devel-5.5.14-77.15.1
php5-sysvmsg-debuginfo-5.5.14-77.15.1
php5-ctype-debuginfo-5.5.14-77.15.1
php5-openssl-5.5.14-77.15.1
php5-pcntl-5.5.14-77.15.1
php5-mbstring-debuginfo-5.5.14-77.15.1
php5-pgsql-debuginfo-5.5.14-77.15.1
php5-pspell-debuginfo-5.5.14-77.15.1
php5-mbstring-5.5.14-77.15.1
php5-iconv-debuginfo-5.5.14-77.15.1
php5-curl-debuginfo-5.5.14-77.15.1
php5-ldap-5.5.14-77.15.1
apache2-mod_php5-debuginfo-5.5.14-77.15.1
php5-tidy-5.5.14-77.15.1
php5-phar-debuginfo-5.5.14-77.15.1
php5-openssl-debuginfo-5.5.14-77.15.1
php5-sockets-debuginfo-5.5.14-77.15.1
php5-fileinfo-5.5.14-77.15.1
php5-pdo-debuginfo-5.5.14-77.15.1
php5-imap-debuginfo-5.5.14-77.15.1
php5-exif-5.5.14-77.15.1
php5-sockets-5.5.14-77.15.1
php5-debugsource-5.5.14-77.15.1
php5-gd-debuginfo-5.5.14-77.15.1
php5-shmop-debuginfo-5.5.14-77.15.1
php5-enchant-debuginfo-5.5.14-77.15.1
php5-snmp-5.5.14-77.15.1
php5-imap-5.5.14-77.15.1
php5-xsl-debuginfo-5.5.14-77.15.1
php5-calendar-debuginfo-5.5.14-77.15.1
php5-shmop-5.5.14-77.15.1
php5-intl-5.5.14-77.15.1
php5-mysql-5.5.14-77.15.1
php5-gmp-5.5.14-77.15.1
php5-odbc-5.5.14-77.15.1
php5-bz2-5.5.14-77.15.1
php5-xmlreader-5.5.14-77.15.1
php5-posix-debuginfo-5.5.14-77.15.1
php5-mssql-5.5.14-77.15.1
php5-pgsql-5.5.14-77.15.1
php5-sysvmsg-5.5.14-77.15.1
php5-xmlreader-debuginfo-5.5.14-77.15.1
php5-json-5.5.14-77.15.1
php5-bz2-debuginfo-5.5.14-77.15.1
php5-zlib-5.5.14-77.15.1
php5-sysvsem-5.5.14-77.15.1

php5-sqlite-debuginfo-5.5.14-77.15.1
php5-sqlite-5.5.14-77.15.1
php5-readline-5.5.14-77.15.1
php5-ftp-5.5.14-77.15.1
php5-firebird-debuginfo-5.5.14-77.15.1
php5-dom-5.5.14-77.15.1
php5-ctype-5.5.14-77.15.1
php5-fpm-debuginfo-5.5.14-77.15.1
php5-gmp-debuginfo-5.5.14-77.15.1
php5-firebird-5.5.14-77.15.1
php5-soap-5.5.14-77.15.1
php5-xsl-5.5.14-77.15.1
php5-enchant-5.5.14-77.15.1
php5-debuginfo-5.5.14-77.15.1
php5-soap-debuginfo-5.5.14-77.15.1
php5-exif-debuginfo-5.5.14-77.15.1
php5-dom-debuginfo-5.5.14-77.15.1
php5-odbc-debuginfo-5.5.14-77.15.1
php5-5.5.14-77.15.1
php5-fileinfo-debuginfo-5.5.14-77.15.1
php5-bcmath-debuginfo-5.5.14-77.15.1
php5-json-debuginfo-5.5.14-77.15.1
php5-curl-5.5.14-77.15.1
php5-wddx-5.5.14-77.15.1
php5-opcache-debuginfo-5.5.14-77.15.1
php5-snmp-debuginfo-5.5.14-77.15.1
php5-sysvsem-debuginfo-5.5.14-77.15.1
php5-pcntl-debuginfo-5.5.14-77.15.1
php5-tidy-debuginfo-5.5.14-77.15.1
php5-suhosin-debuginfo-5.5.14-77.15.1
php5-fastcgi-debuginfo-5.5.14-77.15.1
php5-mssql-debuginfo-5.5.14-77.15.1
php5-mcrypt-debuginfo-5.5.14-77.15.1
php5-mysql-debuginfo-5.5.14-77.15.1
php5-pspell-5.5.14-77.15.1
php5-xmlrpc-debuginfo-5.5.14-77.15.1
apache2-mod_php5-5.5.14-77.15.1

SuSE Linux 42.3
i586
php5-openssl-debuginfo-5.5.14-88.1

146164 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3355-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-17458

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3355-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.opensuse.org/opensuse-updates/2017-12/msg00071.html

SuSE Linux 42.2
i586
mercurial-debugsource-3.8.3-2.11.1
mercurial-3.8.3-2.11.1
mercurial-debuginfo-3.8.3-2.11.1

noarch
mercurial-lang-3.8.3-2.11.1

x86_64
mercurial-debugsource-3.8.3-2.11.1
mercurial-3.8.3-2.11.1
mercurial-debuginfo-3.8.3-2.11.1

SuSE Linux 42.3
i586
mercurial-4.2.3-7.1
mercurial-debugsource-4.2.3-7.1
mercurial-debuginfo-4.2.3-7.1

noarch
mercurial-lang-4.2.3-7.1

x86_64
mercurial-4.2.3-7.1
mercurial-debugsource-4.2.3-7.1
mercurial-debuginfo-4.2.3-7.1

146165 - SuSE Linux 42.3 openSUSE-SU-2017:3359-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-1000410, CVE-2017-11600, CVE-2017-12193, CVE-2017-15115, CVE-2017-16528, CVE-2017-16536, CVE-2017-16537, CVE-2017-16645, CVE-2017-16646, CVE-2017-16939, CVE-2017-16994, CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-7482, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3359-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.opensuse.org/opensuse-updates/2017-12/msg00075.html

SuSE Linux 42.3
x86_64
kselftests-kmp-default-debuginfo-4.4.103-36.1
kernel-debug-base-debuginfo-4.4.103-36.1
kernel-vanilla-devel-4.4.103-36.1
kernel-default-4.4.103-36.1
kselftests-kmp-vanilla-4.4.103-36.1
kernel-default-debugsource-4.4.103-36.1
kernel-default-base-4.4.103-36.1
kernel-obs-build-debugsource-4.4.103-36.1
kselftests-kmp-debug-debuginfo-4.4.103-36.1
kernel-default-devel-4.4.103-36.1

kernel-default-debuginfo-4.4.103-36.1
kernel-vanilla-base-4.4.103-36.1
kernel-vanilla-4.4.103-36.1
kernel-debug-devel-debuginfo-4.4.103-36.1
kernel-syms-4.4.103-36.1
kernel-default-base-debuginfo-4.4.103-36.1
kernel-vanilla-base-debuginfo-4.4.103-36.1
kselftests-kmp-debug-4.4.103-36.1
kernel-debug-debuginfo-4.4.103-36.1
kernel-debug-devel-4.4.103-36.1
kernel-obs-qa-4.4.103-36.1
kernel-debug-debugsource-4.4.103-36.1
kernel-obs-build-4.4.103-36.1
kselftests-kmp-vanilla-debuginfo-4.4.103-36.1
kernel-vanilla-debugsource-4.4.103-36.1
kernel-debug-base-4.4.103-36.1
kernel-debug-4.4.103-36.1
kselftests-kmp-default-4.4.103-36.1
kernel-vanilla-debuginfo-4.4.103-36.1

noarch
kernel-docs-html-4.4.103-36.1
kernel-macros-4.4.103-36.1
kernel-source-vanilla-4.4.103-36.1
kernel-docs-4.4.103-36.1
kernel-docs-pdf-4.4.103-36.1
kernel-devel-4.4.103-36.1
kernel-source-4.4.103-36.1

146166 - SuSE Linux 42.2 openSUSE-SU-2017:3358-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-1000410, CVE-2017-11600, CVE-2017-12193, CVE-2017-15115, CVE-2017-16528, CVE-2017-16536, CVE-2017-16537, CVE-2017-16645, CVE-2017-16646, CVE-2017-16939, CVE-2017-16994, CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-7482, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3358-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.opensuse.org/opensuse-updates/2017-12/msg00074.html

SuSE Linux 42.2
x86_64
kernel-vanilla-debugsource-4.4.103-18.41.1
kernel-vanilla-4.4.103-18.41.1
kernel-debug-devel-debuginfo-4.4.103-18.41.1
kernel-default-debugsource-4.4.103-18.41.1
kernel-obs-qa-4.4.103-18.41.1
kernel-obs-build-debugsource-4.4.103-18.41.1
kernel-default-4.4.103-18.41.1
kernel-debug-base-debuginfo-4.4.103-18.41.1
kernel-debug-base-4.4.103-18.41.1

kernel-default-base-debuginfo-4.4.103-18.41.1
kernel-default-base-4.4.103-18.41.1
kernel-vanilla-devel-4.4.103-18.41.1
kernel-obs-build-4.4.103-18.41.1
kernel-vanilla-base-debuginfo-4.4.103-18.41.1
kernel-syms-4.4.103-18.41.1
kernel-vanilla-debuginfo-4.4.103-18.41.1
kernel-debug-debuginfo-4.4.103-18.41.1
kernel-debug-debugsource-4.4.103-18.41.1
kernel-default-debuginfo-4.4.103-18.41.1
kernel-debug-4.4.103-18.41.1
kernel-debug-devel-4.4.103-18.41.1
kernel-default-devel-4.4.103-18.41.1
kernel-vanilla-base-4.4.103-18.41.1

noarch
kernel-docs-html-4.4.103-18.41.1
kernel-docs-pdf-4.4.103-18.41.1
kernel-macros-4.4.103-18.41.1
kernel-docs-4.4.103-18.41.1
kernel-source-4.4.103-18.41.1
kernel-source-vanilla-4.4.103-18.41.1
kernel-devel-4.4.103-18.41.1

146167 - SuSE SLES 11 SP4 SUSE-SU-2017:3276-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2011-5174

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3276-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003490.html

SuSE SLES 11 SP4
noarch
intel-SINIT-1-0.81.3.2

146168 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3343-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-3737, CVE-2017-3738

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3343-1

Observation

Updates often remediate critical security problems that should be quickly addressed.

For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003538.html

SuSE SLES 12 SP2
noarch
openssl-doc-1.0.2j-60.20.2

x86_64
libopenssl1_0_0-1.0.2j-60.20.2
libopenssl1_0_0-32bit-1.0.2j-60.20.2
libopenssl1_0_0-hmac-1.0.2j-60.20.2
libopenssl1_0_0-debuginfo-32bit-1.0.2j-60.20.2
libopenssl-devel-1.0.2j-60.20.2
libopenssl1_0_0-hmac-32bit-1.0.2j-60.20.2
openssl-debuginfo-1.0.2j-60.20.2
libopenssl1_0_0-debuginfo-1.0.2j-60.20.2
openssl-debugsource-1.0.2j-60.20.2
openssl-1.0.2j-60.20.2

SuSE SLED 12 SP3
x86_64
libopenssl1_0_0-1.0.2j-60.20.2
libopenssl1_0_0-32bit-1.0.2j-60.20.2
libopenssl1_0_0-debuginfo-32bit-1.0.2j-60.20.2
libopenssl-devel-1.0.2j-60.20.2
openssl-debuginfo-1.0.2j-60.20.2
libopenssl1_0_0-debuginfo-1.0.2j-60.20.2
openssl-debugsource-1.0.2j-60.20.2
openssl-1.0.2j-60.20.2

SuSE SLED 12 SP2
x86_64
libopenssl1_0_0-1.0.2j-60.20.2
libopenssl1_0_0-32bit-1.0.2j-60.20.2
libopenssl1_0_0-debuginfo-32bit-1.0.2j-60.20.2
libopenssl-devel-1.0.2j-60.20.2
openssl-debuginfo-1.0.2j-60.20.2
libopenssl1_0_0-debuginfo-1.0.2j-60.20.2
openssl-debugsource-1.0.2j-60.20.2
openssl-1.0.2j-60.20.2

SuSE SLES 12 SP3
noarch
openssl-doc-1.0.2j-60.20.2

x86_64
libopenssl1_0_0-1.0.2j-60.20.2
libopenssl1_0_0-32bit-1.0.2j-60.20.2
libopenssl1_0_0-hmac-1.0.2j-60.20.2
libopenssl1_0_0-debuginfo-32bit-1.0.2j-60.20.2
libopenssl-devel-1.0.2j-60.20.2
libopenssl1_0_0-hmac-32bit-1.0.2j-60.20.2
openssl-debuginfo-1.0.2j-60.20.2
libopenssl1_0_0-debuginfo-1.0.2j-60.20.2
openssl-debugsource-1.0.2j-60.20.2
openssl-1.0.2j-60.20.2

146169 - SuSE Linux 42.3 openSUSE-SU-2017:3363-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-15120

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3363-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.opensuse.org/opensuse-updates/2017-12/msg00077.html

SuSE Linux 42.3
x86_64
pdns-recursor-debugsource-4.0.5-6.1
pdns-recursor-4.0.5-6.1
pdns-recursor-debuginfo-4.0.5-6.1

146170 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3362-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-0741, CVE-2016-4992, CVE-2016-5405, CVE-2017-2591, CVE-2017-2668, CVE-2017-7551

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3362-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.opensuse.org/opensuse-updates/2017-12/msg00076.html

SuSE Linux 42.2
x86_64
389-ds-debugsource-1.3.4.5-5.5.1
389-ds-1.3.4.5-5.5.1
389-ds-debuginfo-1.3.4.5-5.5.1
389-ds-devel-1.3.4.5-5.5.1

i586
389-ds-debugsource-1.3.4.5-5.5.1
389-ds-1.3.4.5-5.5.1
389-ds-debuginfo-1.3.4.5-5.5.1
389-ds-devel-1.3.4.5-5.5.1

SuSE Linux 42.3
x86_64
389-ds-debugsource-1.3.4.5-8.1
389-ds-debuginfo-1.3.4.5-8.1
389-ds-devel-1.3.4.5-8.1
389-ds-1.3.4.5-8.1

i586
389-ds-debugsource-1.3.4.5-8.1
389-ds-debuginfo-1.3.4.5-8.1
389-ds-devel-1.3.4.5-8.1
389-ds-1.3.4.5-8.1

146171 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3346-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-15429

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3346-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.opensuse.org/opensuse-updates/2017-12/msg00062.html

SuSE Linux 42.2
x86_64
chromedriver-debuginfo-63.0.3239.108-104.44.1
chromium-63.0.3239.108-104.44.1
chromedriver-63.0.3239.108-104.44.1
chromium-debuginfo-63.0.3239.108-104.44.1
chromium-debugsource-63.0.3239.108-104.44.1

SuSE Linux 42.3
x86_64
chromedriver-debuginfo-63.0.3239.108-130.1
chromium-debugsource-63.0.3239.108-130.1
chromium-63.0.3239.108-130.1
chromedriver-63.0.3239.108-130.1
chromium-debuginfo-63.0.3239.108-130.1

146173 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3345-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-3737, CVE-2017-3738

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3345-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.opensuse.org/opensuse-updates/2017-12/msg00061.html

SuSE Linux 42.2
i586

openssl-debugsource-1.0.2j-6.9.1
libopenssl1_0_0-hmac-1.0.2j-6.9.1
libopenssl1_0_0-1.0.2j-6.9.1
openssl-debuginfo-1.0.2j-6.9.1
libopenssl1_0_0-debuginfo-1.0.2j-6.9.1
libopenssl-devel-1.0.2j-6.9.1
openssl-cavs-1.0.2j-6.9.1
openssl-cavs-debuginfo-1.0.2j-6.9.1
openssl-1.0.2j-6.9.1

noarch
openssl-doc-1.0.2j-6.9.1

x86_64
libopenssl1_0_0-debuginfo-32bit-1.0.2j-6.9.1
openssl-cavs-debuginfo-1.0.2j-6.9.1
openssl-debuginfo-1.0.2j-6.9.1
openssl-debugsource-1.0.2j-6.9.1
libopenssl1_0_0-1.0.2j-6.9.1
libopenssl-devel-1.0.2j-6.9.1
libopenssl-devel-32bit-1.0.2j-6.9.1
openssl-cavs-1.0.2j-6.9.1
libopenssl1_0_0-hmac-32bit-1.0.2j-6.9.1
libopenssl1_0_0-hmac-1.0.2j-6.9.1
libopenssl1_0_0-32bit-1.0.2j-6.9.1
openssl-1.0.2j-6.9.1
libopenssl1_0_0-debuginfo-1.0.2j-6.9.1

SuSE Linux 42.3
i586
openssl-debugsource-1.0.2j-16.1
libopenssl-devel-1.0.2j-16.1
libopenssl1_0_0-hmac-1.0.2j-16.1
openssl-cavs-1.0.2j-16.1
openssl-1.0.2j-16.1
openssl-cavs-debuginfo-1.0.2j-16.1
libopenssl1_0_0-debuginfo-1.0.2j-16.1
openssl-debuginfo-1.0.2j-16.1
libopenssl1_0_0-1.0.2j-16.1

noarch
openssl-doc-1.0.2j-16.1

x86_64
openssl-debugsource-1.0.2j-16.1
libopenssl1_0_0-hmac-1.0.2j-16.1
libopenssl1_0_0-debuginfo-1.0.2j-16.1
openssl-cavs-1.0.2j-16.1
openssl-1.0.2j-16.1
libopenssl-devel-1.0.2j-16.1
openssl-cavs-debuginfo-1.0.2j-16.1
libopenssl1_0_0-debuginfo-32bit-1.0.2j-16.1
openssl-debuginfo-1.0.2j-16.1
libopenssl1_0_0-32bit-1.0.2j-16.1
libopenssl1_0_0-1.0.2j-16.1
libopenssl-devel-32bit-1.0.2j-16.1
libopenssl1_0_0-hmac-32bit-1.0.2j-16.1

175301 - Scientific Linux Security ERRATA Moderate: postgresql on SL7.x x86_64 (1712-9502)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes

Risk Level: High

CVE: CVE-2017-12172, CVE-2017-15097

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: postgresql on SL7.x x86_64 (1712-9502)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1712&L=scientific-linux-errata&F=&S=&P=9502

SL7
x86_64
postgresql-test-9.2.23-3.el7_4
postgresql-docs-9.2.23-3.el7_4
postgresql-upgrade-9.2.23-3.el7_4
postgresql-plpython-9.2.23-3.el7_4
postgresql-libs-9.2.23-3.el7_4
postgresql-static-9.2.23-3.el7_4
postgresql-9.2.23-3.el7_4
postgresql-contrib-9.2.23-3.el7_4
postgresql-devel-9.2.23-3.el7_4
postgresql-plperl-9.2.23-3.el7_4
postgresql-server-9.2.23-3.el7_4
postgresql-pltcl-9.2.23-3.el7_4
postgresql-debuginfo-9.2.23-3.el7_4

178561 - Gentoo Linux GLSA-201712-02 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: High

CVE: CVE-2017-12597, CVE-2017-12598, CVE-2017-12599, CVE-2017-12600, CVE-2017-12601, CVE-2017-12602, CVE-2017-12603, CVE-2017-12604, CVE-2017-12605, CVE-2017-12606, CVE-2017-12862, CVE-2017-12863, CVE-2017-12864, CVE-2017-14136

Description

The scan detected that the host is missing the following update:
GLSA-201712-02

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://security.gentoo.org/glsa/201712-02

Affected packages:
media-libs/opencv < 2.4.13-r3

186019 - Ubuntu Linux 16.04 USN-3509-3 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-12193, CVE-2017-16643, CVE-2017-16939

Description

The scan detected that the host is missing the following update:
USN-3509-3

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-December/004196.html

Ubuntu 16.04

linux-image-powerpc64-smp_4.4.0.104.109
linux-image-generic_4.4.0.104.109
linux-image-4.4.0-1044-aws_4.4.0-1044.53
linux-image-4.4.0-104-powerpc64-emb_4.4.0-104.127
linux-image-powerpc-smp_4.4.0.104.109
linux-image-4.4.0-104-powerpc64-smp_4.4.0-104.127
linux-image-4.4.0-104-lowlatency_4.4.0-104.127
linux-image-aws_4.4.0.1044.46
linux-image-kvm_4.4.0.1013.13
linux-image-generic-lpae_4.4.0.104.109
linux-image-powerpc64-emb_4.4.0.104.109
linux-image-4.4.0-104-generic-lpae_4.4.0-104.127
linux-image-4.4.0-1013-kvm_4.4.0-1013.18
linux-image-4.4.0-1080-raspi2_4.4.0-1080.88
linux-image-4.4.0-104-powerpc-smp_4.4.0-104.127
linux-image-4.4.0-104-generic_4.4.0-104.127
linux-image-4.4.0-104-powerpc-e500mc_4.4.0-104.127
linux-image-powerpc-e500mc_4.4.0.104.109
linux-image-lowlatency_4.4.0.104.109
linux-image-raspi2_4.4.0.1080.80

186021 - Ubuntu Linux 14.04 USN-3509-4 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-12193, CVE-2017-16643, CVE-2017-16939

Description

The scan detected that the host is missing the following update:
USN-3509-4

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.ubuntu.com/archives/ubuntu-security-announce/2017-December/004197.html

Ubuntu 14.04

linux-image-lowlatency-lts-xenial_4.4.0.104.87
linux-image-4.4.0-104-generic-lpae_4.4.0-104.127~14.04.1
linux-image-powerpc-e500mc-lts-xenial_4.4.0.104.87
linux-image-4.4.0-1006-aws_4.4.0-1006.6

linux-image-4.4.0-104-powerpc-smp_4.4.0-104.127~14.04.1
linux-image-aws_4.4.0.1006.6
linux-image-4.4.0-104-powerpc-e500mc_4.4.0-104.127~14.04.1
linux-image-4.4.0-104-generic_4.4.0-104.127~14.04.1
linux-image-4.4.0-104-powerpc64-emb_4.4.0-104.127~14.04.1
linux-image-4.4.0-104-powerpc64-smp_4.4.0-104.127~14.04.1
linux-image-powerpc64-emb-lts-xenial_4.4.0.104.87
linux-image-generic-lpae-lts-xenial_4.4.0.104.87
linux-image-powerpc64-smp-lts-xenial_4.4.0.104.87
linux-image-powerpc-smp-lts-xenial_4.4.0.104.87
linux-image-4.4.0-104-lowlatency_4.4.0-104.127~14.04.1
linux-image-generic-lts-xenial_4.4.0.104.87

193087 - Fedora Linux 27 FEDORA-2017-a41f6a8078 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-1000158

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a41f6a8078

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

python34-3.4.7-2.fc27

193089 - Fedora Linux 27 FEDORA-2017-677069c484 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-1000158

Description

The scan detected that the host is missing the following update:
FEDORA-2017-677069c484

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 27

python26-2.6.9-10.fc27

193091 - Fedora Linux 26 FEDORA-2017-cf8c62747a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-1000158

Description

The scan detected that the host is missing the following update:
FEDORA-2017-cf8c62747a

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 26

python35-3.5.4-2.fc26

193092 - Fedora Linux 27 FEDORA-2017-fb5e227432 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-15804, CVE-2017-17426

Description

The scan detected that the host is missing the following update:
FEDORA-2017-fb5e227432

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

glibc-2.26-20.fc27

193093 - Fedora Linux 27 FEDORA-2017-99d12bf610 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-1000158

Description

The scan detected that the host is missing the following update:
FEDORA-2017-99d12bf610

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

python35-3.5.4-2.fc27

193097 - Fedora Linux 26 FEDORA-2017-2d441a1d98 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-1000158

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2d441a1d98

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 26

python26-2.6.9-7.fc26

193102 - Fedora Linux 26 FEDORA-2017-e0abe14016 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-1000158

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e0abe14016

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 26

python34-3.4.7-2.fc26

193104 - Fedora Linux 27 FEDORA-2017-5945560816 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-15595, CVE-2017-17563, CVE-2017-17564, CVE-2017-17565, CVE-2017-17566

Description

The scan detected that the host is missing the following update:
FEDORA-2017-5945560816

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

xen-4.9.1-4.fc27

193105 - Fedora Linux 27 FEDORA-2017-5dd9b12179 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-16228

Description

The scan detected that the host is missing the following update:
FEDORA-2017-5dd9b12179

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 27

python-dulwich-0.18.6-1.fc27

22840 - Cisco NX-OS Software Patch Installation Command Injection Vulnerability (cisco-sa-20171129-nxos8)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-12341

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS is a network operating system.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the command line interface (CLI). Successful exploitation could allow a local attacker to perform a command injection attack.

178564 - Gentoo Linux GLSA-201712-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2017-13783, CVE-2017-13784, CVE-2017-13785, CVE-2017-13788, CVE-2017-13791, CVE-2017-13792, CVE-2017-13793, CVE-2017-13794, CVE-2017-13795, CVE-2017-13796, CVE-2017-13798, CVE-2017-13802, CVE-2017-13803

Description

The scan detected that the host is missing the following update:
GLSA-201712-01

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://security.gentoo.org/glsa/201712-01

Affected packages:
net-libs/webkit-gtk < 2.18.3

182553 - FreeBSD libxml2 Multiple Issues (76e59f55-4f7a-4887-bcb0-11604004163a)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-8872, CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050

Description

The scan detected that the host is missing the following update:
libxml2 -- Multiple Issues (76e59f55-4f7a-4887-bcb0-11604004163a)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/76e59f55-4f7a-4887-bcb0-11604004163a.html

Affected packages:
libxml2 <= 2.9.4

193100 - Fedora Linux 26 FEDORA-2017-018464cbf9 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-1000229, CVE-2017-16938

Description

The scan detected that the host is missing the following update:
FEDORA-2017-018464cbf9

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 26

optipng-0.7.6-6.fc26

193103 - Fedora Linux 27 FEDORA-2017-e56a2ddd09 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-1000229, CVE-2017-16938

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e56a2ddd09

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 27

optipng-0.7.6-5.fc27

22809 - (K31300371) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-4483

Description

A denial of service vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP Products are network appliances that run F5's Traffic Management Operating System.

A denial of service vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the Linux kernel. Successful exploitation could allow an attacker to cause a denial of service condition in the target system.

22828 - Cisco NX-OS Software Image Signature Bypass Vulnerability (cisco-sa-20171129-nxos2)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-12333

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS is a network operating system.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to insufficient NX-OS signature verification for software images. Successful exploitation could allow a remote attacker to load a software image bypassing such security mechanism.

22848 - Cisco NX-OS Software Patch Installation Arbitrary File Write Vulnerability (cisco-sa-20171129-nxos1)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-12332

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS is a network operating system .

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in Software patch installation of Cisco NX-OS System. Successful exploitation could allow a local attacker to bypass the security restrictions.

22862 - Cisco NX-OS Software Interactive TCL Shell Escape Vulnerability (cisco-sa-20171129-nxos5)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-12336

Description

A vulnerability is present in some versions of Cisco NX-OS.

Observation

Cisco NX-OS is a network operating system.

A vulnerability is present in some versions of Cisco NX-OS. The flaw lies in the TCL scripting subsystem. Successful exploitation could allow an attacker to gain unauthorized access to the target system and execute arbitrary commands there.

22863 - Cisco NX-OS Software CLI Command Injection Vulnerability (cisco-sa-20171129-nxos4)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-12335

Description

A vulnerability is present in some versions of Cisco NX-OS.

Observation

Cisco NX-OS is a network operating system.

A vulnerability is present in some versions of Cisco NX-OS. The flaw is related with a bad input validation of command arguments. Successful exploitation could allow an attacker to gain unauthorized access to the target system and execute arbitrary commands there.

178562 - Gentoo Linux GLSA-201712-04 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201712-04

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://security.gentoo.org/glsa/201712-04

Affected packages:
net-misc/curl < 7.57.0

178563 - Gentoo Linux GLSA-201712-03 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201712-03

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://security.gentoo.org/glsa/201712-03

Affected packages:
dev-libs/openssl < 1.0.2n

182552 - FreeBSD libXcursor Integer Overflow That Can Lead To Heap Buffer Overflow (ddecde18-e33b-11e7-a293-54e1ad3d6335)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-16612

Description

The scan detected that the host is missing the following update:
libXcursor -- integer overflow that can lead to heap buffer overflow (ddecde18-e33b-11e7-a293-54e1ad3d6335)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/ddecde18-e33b-11e7-a293-54e1ad3d6335.html

Affected packages:
libXcursor < 1.1.15

22855 - Cisco Nexus 7000 Series and Nexus 7700 Series Switches Bash Shell Unauthorized Access Vulnerability (cisco-sa-20171129-switch)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-12340

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS is a network operating system.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the Python scripting sandbox. Successful exploitation could allow a local attacker to escape the Python scripting sandbox and enter the Bash shell.

146163 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3357-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-14042, CVE-2017-14504, CVE-2017-15277, CVE-2017-17498

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3357-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.opensuse.org/opensuse-updates/2017-12/msg00073.html

SuSE Linux 42.2
x86_64
GraphicsMagick-1.3.25-11.52.1
GraphicsMagick-debuginfo-1.3.25-11.52.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.52.1
libGraphicsMagick-Q16-3-1.3.25-11.52.1
GraphicsMagick-devel-1.3.25-11.52.1
perl-GraphicsMagick-debuginfo-1.3.25-11.52.1
libGraphicsMagick++-devel-1.3.25-11.52.1
GraphicsMagick-debugsource-1.3.25-11.52.1
perl-GraphicsMagick-1.3.25-11.52.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.52.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.52.1
libGraphicsMagickWand-Q16-2-1.3.25-11.52.1
libGraphicsMagick++-Q16-12-1.3.25-11.52.1
libGraphicsMagick3-config-1.3.25-11.52.1

i586
GraphicsMagick-1.3.25-11.52.1
GraphicsMagick-debuginfo-1.3.25-11.52.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-11.52.1
libGraphicsMagick-Q16-3-1.3.25-11.52.1
GraphicsMagick-devel-1.3.25-11.52.1
perl-GraphicsMagick-debuginfo-1.3.25-11.52.1
libGraphicsMagick++-devel-1.3.25-11.52.1
GraphicsMagick-debugsource-1.3.25-11.52.1
perl-GraphicsMagick-1.3.25-11.52.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-11.52.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-11.52.1
libGraphicsMagickWand-Q16-2-1.3.25-11.52.1
libGraphicsMagick++-Q16-12-1.3.25-11.52.1
libGraphicsMagick3-config-1.3.25-11.52.1

SuSE Linux 42.3
x86_64
libGraphicsMagick3-config-1.3.25-50.1
GraphicsMagick-debuginfo-1.3.25-50.1
perl-GraphicsMagick-debuginfo-1.3.25-50.1
GraphicsMagick-1.3.25-50.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-50.1
GraphicsMagick-debugsource-1.3.25-50.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-50.1
libGraphicsMagick++-Q16-12-1.3.25-50.1
GraphicsMagick-devel-1.3.25-50.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-50.1
libGraphicsMagickWand-Q16-2-1.3.25-50.1
libGraphicsMagick++-devel-1.3.25-50.1
perl-GraphicsMagick-1.3.25-50.1
libGraphicsMagick-Q16-3-1.3.25-50.1

i586
libGraphicsMagick3-config-1.3.25-50.1
GraphicsMagick-debuginfo-1.3.25-50.1
perl-GraphicsMagick-debuginfo-1.3.25-50.1
GraphicsMagick-1.3.25-50.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-50.1
GraphicsMagick-debugsource-1.3.25-50.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-50.1
libGraphicsMagick++-Q16-12-1.3.25-50.1
GraphicsMagick-devel-1.3.25-50.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-50.1
libGraphicsMagickWand-Q16-2-1.3.25-50.1
libGraphicsMagick++-devel-1.3.25-50.1
perl-GraphicsMagick-1.3.25-50.1
libGraphicsMagick-Q16-3-1.3.25-50.1

193094 - Fedora Linux 27 FEDORA-2017-874bd165c0 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-10789

Description

The scan detected that the host is missing the following update:
FEDORA-2017-874bd165c0

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 27

perl-DBD-MySQL-4.043-6.fc27

22813 - Cisco NX-OS Software Guest Shell Unauthorized Internal Interface Access Vulnerability (cisco-sa-20171129-nxos10)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2017-12351

Description

A vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS is a network operating system.

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the guest shell feature. Successful exploitation could allow a local attacker to read and send packets outside the scope of the guest shell container.

33377 - Oracle Solaris 119410-10 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
119410-10

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://getupdates.oracle.com/readme/119410-10

GNOME 2.6.0: GNOME Applets Patch

SOLARIS_10

SUNWgnome-fun-applets:2.6.0,REV=10.0.3.2004.12.15.19.13
SUNWgnome-internet-applets:2.6.0,REV=10.0.3.2004.12.15.19.13
SUNWgnome-mm-applets:2.6.0,REV=10.0.3.2004.12.15.19.13
SUNWgnome-intranet-applets-share:2.6.0,REV=10.0.3.2004.12.15.19.13
SUNWgnome-intranet-applets:2.6.0,REV=10.0.3.2004.12.15.19.13
SUNWgnome-utility-applets:2.6.0,REV=10.0.3.2004.12.15.19.14
SUNWgnome-dictionary:2.6.0,REV=10.0.3.2004.12.16.00.58

33378 - Oracle Solaris 119411-10 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
119411-10

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://getupdates.oracle.com/readme/119411-10

GNOME 2.6.0(x86): GNOME Applets Patch

SOLARIS_10_x86

SUNWgnome-fun-applets:2.6.0,REV=10.0.3.2004.12.16.17.46
SUNWgnome-intranet-applets-share:2.6.0,REV=10.0.3.2004.12.16.17.46
SUNWgnome-utility-applets:2.6.0,REV=10.0.3.2004.12.16.17.46
SUNWgnome-internet-applets:2.6.0,REV=10.0.3.2004.12.16.17.46
SUNWgnome-intranet-applets:2.6.0,REV=10.0.3.2004.12.16.17.46
SUNWgnome-mm-applets:2.6.0,REV=10.0.3.2004.12.16.17.46
SUNWgnome-dictionary:2.6.0,REV=10.0.3.2004.12.16.20.27

130973 - Debian Linux 8.0, 9.0 DSA-4067-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-17432

Description

The scan detected that the host is missing the following update:
DSA-4067-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2017/dsa-4067

Debian 8.0
all
openafs-doc_1.6.9-2+deb8u6
openafs-dbg_1.6.9-2+deb8u6
openafs-modules-dkms_1.6.9-2+deb8u6
libafsauthent1_1.6.9-2+deb8u6
openafs-kpasswd_1.6.9-2+deb8u6
libkopenafs1_1.6.9-2+deb8u6
openafs-modules-source_1.6.9-2+deb8u6
openafs-client_1.6.9-2+deb8u6
libopenafs-dev_1.6.9-2+deb8u6
openafs-dbserver_1.6.9-2+deb8u6
openafs-fileserver_1.6.9-2+deb8u6
openafs-krb5_1.6.9-2+deb8u6
openafs-fuse_1.6.9-2+deb8u6
libpam-openafs-kaserver_1.6.9-2+deb8u6
libafsrpc1_1.6.9-2+deb8u6

Debian 9.0
all
libafsauthent1_1.6.20-2+deb9u1
openafs-fuse_1.6.20-2+deb9u1
openafs-doc_1.6.20-2+deb9u1
libopenafs-dev_1.6.20-2+deb9u1
libkopenafs1_1.6.20-2+deb9u1
libafsrpc1_1.6.20-2+deb9u1
openafs-modules-source_1.6.20-2+deb9u1
openafs-fileserver_1.6.20-2+deb9u1

openafs-kpasswd_1.6.20-2+deb9u1
openafs-dbserver_1.6.20-2+deb9u1
openafs-krb5_1.6.20-2+deb9u1
libpam-openafs-kaserver_1.6.20-2+deb9u1
openafs-modules-dkms_1.6.20-2+deb9u1
openafs-client_1.6.20-2+deb9u1

130974 - Debian Linux 9.0 DSA-4065-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-3737, CVE-2017-3738

Description

The scan detected that the host is missing the following update:
DSA-4065-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2017/dsa-4065

Debian 9.0
all
libssl1.0-dev_1.0.2l-2+deb9u2
libssl1.0.2_1.0.2l-2+deb9u2
libcrypto1.0.2-udeb_1.0.2l-2+deb9u2
libssl1.0.2-udeb_1.0.2l-2+deb9u2

130975 - Debian Linux 8.0, 9.0 DSA-4066-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-16854, CVE-2017-16921

Description

The scan detected that the host is missing the following update:
DSA-4066-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.debian.org/security/2017/dsa-4066

Debian 8.0
all
otrs2_3.3.18-1+deb8u3

Debian 9.0
all
otrs2_5.0.16-1+deb9u4

182548 - FreeBSD jenkins Two Startup Race Conditions (7136e6b7-e1b3-11e7-a4d3-000c292ee6b8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
jenkins -- Two startup race conditions (7136e6b7-e1b3-11e7-a4d3-000c292ee6b8)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/7136e6b7-e1b3-11e7-a4d3-000c292ee6b8.html

Affected packages:
jenkins < 2.95
jenkins-lts < 2.89.2

182549 - FreeBSD rubygem-passenger Arbitrary File Read Vulnerability (8cf25a29-e063-11e7-9b2c-001e672571bc)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-16355

Description

The scan detected that the host is missing the following update:
rubygem-passenger -- arbitrary file read vulnerability (8cf25a29-e063-11e7-9b2c-001e672571bc)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/8cf25a29-e063-11e7-9b2c-001e672571bc.html

Affected packages:
5.0.10 <= rubygem-passenger < 5.1.11

182550 - FreeBSD node.js Data Confidentiality/Integrity Vulnerability, December 2017 (bea84a7a-e0c9-11e7-b4f3-11baa0c2df21)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-15896, CVE-2017-15897, CVE-2017-3738

Description

The scan detected that the host is missing the following update:
node.js -- Data Confidentiality/Integrity Vulnerability, December 2017 (bea84a7a-e0c9-11e7-b4f3-11baa0c2df21)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/bea84a7a-e0c9-11e7-b4f3-11baa0c2df21.html

Affected packages:
node4 < 4.8.7
node6 < 6.12.2
node8 < 8.9.3
node < 9.2.1

182551 - FreeBSD tor Use-after-free In Onion Service V2 (36ef8753-d86f-11e7-ad28-0025908740c2)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-8819

Description

The scan detected that the host is missing the following update:
tor -- Use-after-free in onion service v2 (36ef8753-d86f-11e7-ad28-0025908740c2)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/36ef8753-d86f-11e7-ad28-0025908740c2.html

Affected packages:
tor < 0.3.1.9

182554 - FreeBSD global Gozilla Vulnerability (48cca164-e269-11e7-be51-6599c735afc8)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-17531

Description

The scan detected that the host is missing the following update:
global -- gozilla vulnerability (48cca164-e269-11e7-be51-6599c735afc8)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/48cca164-e269-11e7-be51-6599c735afc8.html

Affected packages:
4.8.6 <= global < 6.6.1

182555 - FreeBSD GitLab Multiple Vulnerabilities (e72a8864-e0bc-11e7-b627-d43d7e971a1b)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GitLab -- multiple vulnerabilities (e72a8864-e0bc-11e7-b627-d43d7e971a1b)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/e72a8864-e0bc-11e7-b627-d43d7e971a1b.html

Affected packages:
4.2.0 <= gitlab <= 10.0.6
10.1.0 <= gitlab <= 10.1.4
10.2.0 <= gitlab <= 10.2.3

182556 - FreeBSD asterisk Remote Crash Vulnerability In RTCP Stack (4a67450a-e044-11e7-accc-001999f8d30b)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
asterisk -- Remote Crash Vulnerability in RTCP Stack (4a67450a-e044-11e7-accc-001999f8d30b)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/4a67450a-e044-11e7-accc-001999f8d30b.html

Affected packages:
asterisk13 < 13.18.4

182557 - FreeBSD libXfont Multiple Memory Leaks (3b9590a1-e358-11e7-a293-54e1ad3d6335)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-13720, CVE-2017-13722

Description

The scan detected that the host is missing the following update:
libXfont -- multiple memory leaks (3b9590a1-e358-11e7-a293-54e1ad3d6335)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/3b9590a1-e358-11e7-a293-54e1ad3d6335.html

Affected packages:
libXfont < 1.5.3
libXfont2 < 2.0.2

182558 - FreeBSD libXfont Permission Bypass When Opening Files Through Symlinks (08a125f3-e35a-11e7-a293-54e1ad3d6335)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-16611

Description

The scan detected that the host is missing the following update:
libXfont -- permission bypass when opening files through symlinks (08a125f3-e35a-11e7-a293-54e1ad3d6335)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/08a125f3-e35a-11e7-a293-54e1ad3d6335.html

Affected packages:
libXfont < 1.5.4
libXfont2 < 2.0.3

182559 - FreeBSD ruby Command Injection Vulnerability In Net::FTP (dd644964-e10e-11e7-8097-0800271d4b9c)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-17405

Description

The scan detected that the host is missing the following update:
ruby -- Command injection vulnerability in Net::FTP (dd644964-e10e-11e7-8097-0800271d4b9c)

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://www.vuxml.org/freebsd/dd644964-e10e-11e7-8097-0800271d4b9c.html

Affected packages:
2.2.0,1 <= ruby < 2.2.9,1
2.3.0,1 <= ruby < 2.3.6,1
2.4.0,1 <= ruby < 2.4.3,1

193085 - Fedora Linux 26 FEDORA-2017-e68e87955b Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-16910

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e68e87955b

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 26

LibRaw-0.18.6-1.fc26

193086 - Fedora Linux 27 FEDORA-2017-1682a6a2a0 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2017-1682a6a2a0

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

qt5-qtbase-5.9.2-6.fc27

193088 - Fedora Linux 26 FEDORA-2017-0f3270406c Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-17440

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0f3270406c

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 26

libextractor-1.6-2.fc26

193090 - Fedora Linux 26 FEDORA-2017-bce9e03721 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-8819, CVE-2017-8820, CVE-2017-8821, CVE-2017-8822, CVE-2017-8823

Description

The scan detected that the host is missing the following update:

FEDORA-2017-bce9e03721

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 26

tor-0.3.1.9-1.fc26

193095 - Fedora Linux 27 FEDORA-2017-bc2edc421d Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-8819, CVE-2017-8820, CVE-2017-8821, CVE-2017-8822, CVE-2017-8823

Description

The scan detected that the host is missing the following update:
FEDORA-2017-bc2edc421d

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 27

tor-0.3.1.9-1.fc27

193096 - Fedora Linux 27 FEDORA-2017-e6be32cb7a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e6be32cb7a

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

nodejs-8.9.3-2.fc27

193098 - Fedora Linux 27 FEDORA-2017-b414bd5b99 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b414bd5b99

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

wayland-1.14.0-2.fc27

193099 - Fedora Linux 26 FEDORA-2017-ba6b6e71f7 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-17558, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ba6b6e71f7

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 26

kernel-4.14.6-200.fc26

193101 - Fedora Linux 27 FEDORA-2017-354b9647ba Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-17440

Description

The scan detected that the host is missing the following update:
FEDORA-2017-354b9647ba

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 27

libextractor-1.6-2.fc27

193106 - Fedora Linux 26 FEDORA-2017-aa4cc10bde Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2017-aa4cc10bde

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 26

qt5-qtbase-5.9.2-6.fc26

193107 - Fedora Linux 27 FEDORA-2017-129969aa8a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-17558, CVE-2017-8824

Description

The scan detected that the host is missing the following update:
FEDORA-2017-129969aa8a

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=2

Fedora Core 27

kernel-4.14.6-300.fc27

193108 - Fedora Linux 26 FEDORA-2017-26c3ab48e4 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2017-26c3ab48e4

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2017/12/?count=200&page=1

Fedora Core 26

wayland-1.13.0-3.fc26

146161 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3325-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-12618

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3325-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.opensuse.org/opensuse-updates/2017-12/msg00051.html

SuSE Linux 42.2
x86_64
libapr-util1-dbd-pgsql-1.5.3-5.3.1
libapr-util1-debuginfo-1.5.3-5.3.1
libapr-util1-dbd-mysql-1.5.3-5.3.1
libapr-util1-devel-1.5.3-5.3.1
libapr-util1-dbd-sqlite3-1.5.3-5.3.1
libapr-util1-dbd-pgsql-debuginfo-1.5.3-5.3.1
libapr-util1-1.5.3-5.3.1
libapr-util1-dbd-mysql-debuginfo-1.5.3-5.3.1
libapr-util1-debugsource-1.5.3-5.3.1
libapr-util1-dbd-sqlite3-debuginfo-1.5.3-5.3.1

i586
libapr-util1-dbd-pgsql-1.5.3-5.3.1
libapr-util1-debuginfo-1.5.3-5.3.1
libapr-util1-dbd-mysql-1.5.3-5.3.1
libapr-util1-devel-1.5.3-5.3.1
libapr-util1-dbd-sqlite3-1.5.3-5.3.1
libapr-util1-dbd-pgsql-debuginfo-1.5.3-5.3.1
libapr-util1-1.5.3-5.3.1
libapr-util1-dbd-mysql-debuginfo-1.5.3-5.3.1
libapr-util1-debugsource-1.5.3-5.3.1
libapr-util1-dbd-sqlite3-debuginfo-1.5.3-5.3.1

SuSE Linux 42.3
x86_64
libapr-util1-1.5.3-8.1
libapr-util1-dbd-mysql-1.5.3-8.1
libapr-util1-dbd-pgsql-1.5.3-8.1
libapr-util1-debugsource-1.5.3-8.1
libapr-util1-dbd-pgsql-debuginfo-1.5.3-8.1
libapr-util1-dbd-sqlite3-debuginfo-1.5.3-8.1

libapr-util1-devel-1.5.3-8.1
libapr-util1-debuginfo-1.5.3-8.1
libapr-util1-dbd-mysql-debuginfo-1.5.3-8.1
libapr-util1-dbd-sqlite3-1.5.3-8.1

i586
libapr-util1-1.5.3-8.1
libapr-util1-dbd-mysql-1.5.3-8.1
libapr-util1-dbd-pgsql-1.5.3-8.1
libapr-util1-debugsource-1.5.3-8.1
libapr-util1-dbd-pgsql-debuginfo-1.5.3-8.1
libapr-util1-dbd-sqlite3-debuginfo-1.5.3-8.1
libapr-util1-devel-1.5.3-8.1
libapr-util1-debuginfo-1.5.3-8.1
libapr-util1-dbd-mysql-debuginfo-1.5.3-8.1
libapr-util1-dbd-sqlite3-1.5.3-8.1

146172 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:3278-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-12618

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3278-1

Observation

Updates often remediate critical security problems that should be quickly addressed.
For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2017-December/003492.html

SuSE SLES 12 SP3
x86_64
libapr-util1-dbd-sqlite3-debuginfo-1.5.3-2.3.1
libapr-util1-dbd-sqlite3-1.5.3-2.3.1
libapr-util1-debuginfo-1.5.3-2.3.1
libapr-util1-1.5.3-2.3.1
libapr-util1-debugsource-1.5.3-2.3.1

SuSE SLES 12 SP2
x86_64
libapr-util1-dbd-sqlite3-debuginfo-1.5.3-2.3.1
libapr-util1-dbd-sqlite3-1.5.3-2.3.1
libapr-util1-debuginfo-1.5.3-2.3.1
libapr-util1-1.5.3-2.3.1
libapr-util1-debugsource-1.5.3-2.3.1

22867 - TLS RSA Key Exchange Algorithm Detected

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

TLS RSA key exchange algorithm was detected on the host.

Observation

TLS supports a wide variety of algorithms used for encryption and decryption called ciphers thus allowing users to select different security levels.

TLS RSA key exchange algorithm was detected on the host.

Make sure TLS RSA key exchange algorithm implementation is correct to avoid issue such as Bleichenbacher's Oracle Threat and the new Robot Attack.

ENHANCED CHECKS

The following checks have been updated. Enhancements may include optimizations, changes that reflect new information on a vulnerability and anything else that improves upon an existing FSL check.

21831 - WordPress Multiple Vulnerabilities Prior To 4.7.5

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: High

CVE: CVE-2017-9061, CVE-2017-9062, CVE-2017-9063, CVE-2017-9064, CVE-2017-9065, CVE-2017-9066

Update Details

Name is updated Observation is updated CVE is updated

22451 - (APSB17-28) Vulnerabilities In Adobe Flash Player

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-11281, CVE-2017-11282

Update Details

Risk is updated

22452 - (APSB17-28) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-11281, CVE-2017-11282

Update Details

Risk is updated

22461 - (APSB17-30) Vulnerabilities In Adobe ColdFusion

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-11283, CVE-2017-11284, CVE-2017-11285, CVE-2017-11286

Update Details

Risk is updated

32160 - Oracle Solaris 136882-08 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: High

CVE: CVE-2004-0981, CVE-2005-0397, CVE-2005-0759, CVE-2005-0760, CVE-2005-0761, CVE-2005-0762, CVE-2005-1739, CVE-2005-4601, CVE-2006-0082, CVE-2006-3744, CVE-2007-4985, CVE-2007-4986, CVE-2007-4987, CVE-2007-4988, CVE-2010-4167

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

32163 - Oracle Solaris 136883-08 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: High

CVE: CVE-2004-0981, CVE-2005-0397, CVE-2005-0759, CVE-2005-0760, CVE-2005-0761, CVE-2005-0762, CVE-2005-1739, CVE-2005-4601, CVE-2006-0082, CVE-2006-3744, CVE-2007-4985, CVE-2007-4986, CVE-2007-4987, CVE-2007-4988, CVE-2010-4167

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

88902 - Slackware Linux 14.0, 14.1, 14.2 SSA:2017-333-03 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-8816, CVE-2017-8817, CVE-2017-8818

Update Details

Risk is updated

130959 - Debian Linux 8.0, 9.0 DSA-4051-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-8816, CVE-2017-8817

Update Details

Risk is updated

141704 - Red Hat Enterprise Linux RHSA-2017-2702 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-11281, CVE-2017-11282

Update Details

Risk is updated

182439 - FreeBSD Flash Player Multiple Vulnerabilities (531aae08-97f0-11e7-aadd-6451062f0f7a)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-11281, CVE-2017-11282

Update Details
Risk is updated

182531 - FreeBSD cURL Multiple Vulnerabilities (301a01b7-d50e-11e7-ac58-b499baebfeaf)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-8816, CVE-2017-8817, CVE-2017-8818

Update Details
Risk is updated

185999 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3498-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-8816, CVE-2017-8817

Update Details
Risk is updated

193047 - Fedora Linux 27 FEDORA-2017-4bfcd57172 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-17044, CVE-2017-17045

Update Details
Risk is updated

193058 - Fedora Linux 27 FEDORA-2017-45bdf4dace Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-8816, CVE-2017-8817

Update Details
Risk is updated

193073 - Fedora Linux 26 FEDORA-2017-0c062324cd Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-8816, CVE-2017-8817

Update Details
Risk is updated

182517 - FreeBSD asterisk Buffer Overflow In CDR's Set User (ab04cb0b-c533-11e7-8da5-001999f8d30b)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-16671

Update Details

Risk is updated CVE is updated FASLScript is updated

22480 - (APSB17-25) Vulnerabilities In RoboHelp

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-3104, CVE-2017-3105

Update Details

Risk is updated

22764 - (APSB17-39) Vulnerability In Adobe Digital Editions

Category: Windows Host Assessment -> Adobe Patches Only
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-11273, CVE-2017-11297, CVE-2017-11298, CVE-2017-11299, CVE-2017-11300, CVE-2017-11301

Update Details

Risk is updated

88901 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-333-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-16612

Update Details

Risk is updated

130966 - Debian Linux 8.0, 9.0 DSA-4059-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-16612

Update Details

Risk is updated

146118 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3202-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-17083, CVE-2017-17084, CVE-2017-17085

Update Details

Risk is updated

146128 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3214-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-16612

Update Details

Risk is updated

182547 - FreeBSD wireshark Multiple Security Issues (4b228e69-22e1-4019-afd0-8aa716d0ec0b)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-17083, CVE-2017-17084, CVE-2017-17085

Update Details

Risk is updated

185996 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3501-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-16612

Update Details

Risk is updated

33162 - Oracle Solaris 150400-58 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2004-0230, CVE-2013-5862, CVE-2013-5876, CVE-2014-0447, CVE-2014-6473, CVE-2014-6575, CVE-2015-0375, CVE-2015-0471, CVE-2015-2580, CVE-2015-2589, CVE-2015-4869, CVE-2016-3419, CVE-2016-3441, CVE-2016-3453, CVE-2016-5553, CVE-2017-10004, CVE-2017-10036, CVE-2017-10042, CVE-2017-10122

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

182518 - FreeBSD asterisk Memory/File Descriptor/RTP Leak In Pjsip Session Resource (be261737-c535-11e7-8da5-001999f8d30b)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-16672

Update Details

Risk is updated CVE is updated

33319 - Oracle Solaris 151913-10 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

33323 - Oracle Solaris 151912-10 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Update Details

Name is updated Description is updated Observation is updated Recommendation is updated FASLScript is updated

182534 - FreeBSD asterisk DOS Vulnerability In Asterisk Chan_skinny (e91cf90c-d6dd-11e7-9d10-001999f8d30b)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: Low

CVE: CVE-2017-17090

Update Details

CVE is updated

70116 - scada.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will

be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

http://www.mcafee.com/us/about/contact/index.html

Non-US customers - Select your country from the list of Worldwide Offices.