2017-APR-06
FSL version 7.5.909

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

21538 - ACTi Cameras Information Exposure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: High

CVE: CVE-2017-3185

Description

A vulnerability is present in some firmware versions of ACTi cameras.

Observation

ACTi cameras is a widely spreaded brand of surveillance cameras.

A vulnerability is present in some firmware versions of ACTi cameras. The flaw lies in the web-based user interface, which uses the GET method to process requests that contain sensitive information, like login information. Successful exploitation could allow a malicious user to obtain the access credentials of the device.

21550 - Novell iPrint Appliance Multiple Vulnerabilities Prior To 2.0 Patch 4

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2004-0230, CVE-2012-6704, CVE-2015-1350, CVE-2015-8956, CVE-2015-8962, CVE-2015-8964, CVE-2015-8970, CVE-2016-0823, CVE-2016-1000, CVE-2016-1001, CVE-2016-1008, CVE-2016-1015, CVE-2016-1016, CVE-2016-2108, CVE-2016-3841, CVE-2016-6828, CVE-2016-7042, CVE-2016-7056, CVE-2016-7097, CVE-2016-7117, CVE-2016-7425, CVE-2016-7478, CVE-2016-7910, CVE-2016-7911, CVE-2016-7916, CVE-2016-8399, CVE-2016-8610, CVE-2016-8632, CVE-2016-8633, CVE-2016-8646, CVE-2016-8858, CVE-2016-9555, CVE-2016-9576, CVE-2016-9685, CVE-2016-9756, CVE-2016-9793, CVE-2017-3135, CVE-2017-3731, CVE-2017-5551

Description

Multiple vulnerabilities are present in some versions of Novell iPrint Appliance.

Observation

Novell iPrint Appliance is a popular virtual appliance that offers self-service printing for the enterprises.

Multiple vulnerabilities are present in some versions of Novell iPrint Appliance. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code, bypass security measures, obtain sensitive information or cause a denial of service condition.

21564 - Novell iPrint Appliance Multiple Vulnerabilities Prior To 2.1 Patch 2

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2004-0230, CVE-2012-6704, CVE-2015-1350, CVE-2015-5219, CVE-2015-8139, CVE-2015-8140, CVE-2015-8956, CVE-2015-8962, CVE-2015-8964, CVE-2015-8970, CVE-2016-0823, CVE-2016-1000, CVE-2016-1001, CVE-2016-1008, CVE-2016-1015,

CVE-2016-1016, CVE-2016-2108, CVE-2016-2125, CVE-2016-2126, CVE-2016-3841, CVE-2016-5285, CVE-2016-5290, CVE-2016-5291, CVE-2016-5296, CVE-2016-5297, CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5568, CVE-2016-5573, CVE-2016-5597, CVE-2016-6664, CVE-2016-6828, CVE-2016-7042, CVE-2016-7056, CVE-2016-7097, CVE-2016-7117, CVE-2016-7425, CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-7478, CVE-2016-7910, CVE-2016-7911, CVE-2016-7916, CVE-2016-8399, CVE-2016-8610, CVE-2016-8632, CVE-2016-8633, CVE-2016-8646, CVE-2016-8858, CVE-2016-9064, CVE-2016-9066, CVE-2016-9074, CVE-2016-9079, CVE-2016-9131, CVE-2016-9147, CVE-2016-9168, CVE-2016-9310, CVE-2016-9311, CVE-2016-9444, CVE-2016-9555, CVE-2016-9576, CVE-2016-9685, CVE-2016-9756, CVE-2016-9793, CVE-2016-9794, CVE-2017-3135, CVE-2017-3238, CVE-2017-3243, CVE-2017-3244, CVE-2017-3258, CVE-2017-3265, CVE-2017-3291, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3731, CVE-2017-5551

Description

Multiple vulnerabilities are present in some versions of Novell iPrint Appliance.

Observation

Novell iPrint Appliance is a popular virtual appliance that offers self-service printing for the enterprises.

Multiple vulnerabilities are present in some versions of Novell iPrint Appliance. The flaws lie in several components. Successful exploitation could allow an attacker to obtain elevated privileges or execute arbitrary code affecting confidentiality, availability, and integrity of the system.

132346 - Oracle VM OVMSA-2017-0057 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-0343, CVE-2013-2140, CVE-2013-2147, CVE-2013-2148, CVE-2013-2164, CVE-2013-2234, CVE-2013-2237, CVE-2013-2850, CVE-2013-2851, CVE-2013-2852, CVE-2013-2889, CVE-2013-2895, CVE-2013-2896, CVE-2013-2929, CVE-2013-4162, CVE-2013-4163, CVE-2013-4299, CVE-2013-4312, CVE-2013-4345, CVE-2013-4348, CVE-2013-4350, CVE-2013-4470, CVE-2013-4579, CVE-2013-4587, CVE-2013-4592, CVE-2013-6367, CVE-2013-6368, CVE-2013-6376, CVE-2013-6383, CVE-2013-6885, CVE-2014-0038, CVE-2014-0049, CVE-2014-0055, CVE-2014-0069, CVE-2014-0077, CVE-2014-0101, CVE-2014-0196, CVE-2014-1737, CVE-2014-1738, CVE-2014-1739, CVE-2014-2851, CVE-2014-3144, CVE-2014-3145, CVE-2014-3181, CVE-2014-3182, CVE-2014-3184, CVE-2014-3185, CVE-2014-3215, CVE-2014-3535, CVE-2014-3610, CVE-2014-3611, CVE-2014-3645, CVE-2014-3646, CVE-2014-3687, CVE-2014-3688, CVE-2014-4027, CVE-2014-4652, CVE-2014-4653, CVE-2014-4654, CVE-2014-4655, CVE-2014-4656, CVE-2014-4667, CVE-2014-4943, CVE-2014-5471, CVE-2014-5472, CVE-2014-7822, CVE-2014-7826, CVE-2014-7970, CVE-2014-8133, CVE-2014-8134, CVE-2014-8159, CVE-2014-8160, CVE-2014-8171, CVE-2014-8173, CVE-2014-8884, CVE-2014-8989, CVE-2014-9090, CVE-2014-9585, CVE-2015-0239, CVE-2015-1333, CVE-2015-1421, CVE-2015-1805, CVE-2015-2830, CVE-2015-2922, CVE-2015-3212, CVE-2015-3339, CVE-2015-3636, CVE-2015-5156, CVE-2015-5157, CVE-2015-5283, CVE-2015-5697, CVE-2015-5707, CVE-2015-7613, CVE-2015-7872, CVE-2015-8104, CVE-2015-8374, CVE-2015-8543, CVE-2015-8569, CVE-2016-0728, CVE-2016-0758, CVE-2016-10142, CVE-2016-2053, CVE-2016-3070, CVE-2016-3134, CVE-2016-3140, CVE-2016-3672, CVE-2016-4470, CVE-2016-4482, CVE-2016-4485, CVE-2016-4565, CVE-2016-4569, CVE-2016-4578, CVE-2016-4580, CVE-2016-5195, CVE-2016-6136, CVE-2016-6327, CVE-2016-6480, CVE-2016-6828, CVE-2016-7042, CVE-2016-7117, CVE-2016-7425, CVE-2016-8399, CVE-2016-8633, CVE-2016-8645, CVE-2016-8646, CVE-2016-8650, CVE-2016-8655, CVE-2016-9178, CVE-2016-9555, CVE-2016-9644, CVE-2016-9793, CVE-2016-9794, CVE-2017-2636, CVE-2017-5970, CVE-2017-6345, CVE-2017-7187

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0057

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-April/000675.html

OVM3.3
x86_64
kernel-uek-3.8.13-118.17.4.el6uek
kernel-uek-firmware-3.8.13-118.17.4.el6uek

132353 - Oracle VM OVMSA-2017-0050 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-7169, CVE-2016-0634, CVE-2016-7543, CVE-2016-9401

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0050

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000659.html
http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000669.html

OVM3.3
x86_64
bash-4.1.2-48.el6

OVM3.4
x86_64
bash-4.1.2-48.el6

21537 - ACTi Cameras Missing Authentication for Critical Function Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: High

CVE: CVE-2017-3184

Description

A vulnerability is present in some firmware versions of ACTi cameras.

Observation

ACTi cameras are a widely spreaded brand of surveillance cameras.

A vulnerability is present in some firmware versions of ACTi cameras. The flaw lies in the web-based user interface. Successful exploitation of this vulnerability could allow a malicious user to perform a factory reset, leading to a denial-of-service or allowing the use of default credentials to access the system. Exploitation requires the attacker to access directly to the settings restore module via http://x.x.x.x/setup/setup_maintain_firmware-default.html.

21539 - ACTi Cameras Weak Password Requirements Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: High

CVE: CVE-2017-3186

Description

A vulnerability is present in some firmware versions of ACTi cameras.

Observation

ACTi cameras is a widely spreaded brand of surveillance cameras.

A vulnerability is present in some firmware versions of ACTi cameras. The flaw lies in the authentication subsystem, which uses non-random default credentials across all devices. Successful exploitation could allow an attacker to obtain full control of the affected device.

21561 - (VMSA-2017-0004) VMware vRealize Operations Apache Struts 2 RCE Vulnerability

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

Risk Level: High

CVE: CVE-2017-5638

Description

A vulnerability is present in some versions of VMware vRealize Operations.

Observation

VMware vRealize Operations is the VMware's IT operations management software.

A vulnerability is present in some versions of VMware vRealize Operations. The flaw lies in Apache Struts 2 component. Successful exploitation could allow an attacker to execute remote code.

21562 - (VMSA-2017-0004) VMware vRealize Operations Apache Struts 2 RCE Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-5638

Description

A vulnerability is present in some versions of VMware vRealize Operations.

Observation

VMware vRealize Operations is the VMware's IT operations management software.

A vulnerability is present in some versions of VMware vRealize Operations. The flaw lies in Apache Struts 2 component. Successful exploitation could allow an attacker to execute remote code.

132347 - Oracle VM OVMSA-2017-0056 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8952, CVE-2016-10088, CVE-2016-10147, CVE-2016-3140, CVE-2016-3672, CVE-2016-3951, CVE-2016-7097, CVE-2016-7425, CVE-2016-8399, CVE-2016-8632, CVE-2016-8633, CVE-2016-8645, CVE-2016-9178, CVE-2016-9588, CVE-2016-9644, CVE-2016-9756, CVE-2017-2596, CVE-2017-2636, CVE-2017-5897, CVE-2017-5970, CVE-2017-6001, CVE-2017-6345, CVE-2017-7187

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0056

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-April/000674.html

OVM3.4
x86_64
kernel-uek-firmware-4.1.12-61.1.33.el6uek
kernel-uek-4.1.12-61.1.33.el6uek

141529 - Red Hat Enterprise Linux RHSA-2017-0860 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056

Description

The scan detected that the host is missing the following update:
RHSA-2017-0860

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-March/msg00049.html

RHEL6D
x86_64
chromium-browser-debuginfo-57.0.2987.133-1.el6_9
chromium-browser-57.0.2987.133-1.el6_9

i386
chromium-browser-debuginfo-57.0.2987.133-1.el6_9
chromium-browser-57.0.2987.133-1.el6_9

RHEL6S
x86_64
chromium-browser-debuginfo-57.0.2987.133-1.el6_9
chromium-browser-57.0.2987.133-1.el6_9

i386
chromium-browser-debuginfo-57.0.2987.133-1.el6_9
chromium-browser-57.0.2987.133-1.el6_9

RHEL6WS
x86_64
chromium-browser-debuginfo-57.0.2987.133-1.el6_9
chromium-browser-57.0.2987.133-1.el6_9

i386
chromium-browser-debuginfo-57.0.2987.133-1.el6_9
chromium-browser-57.0.2987.133-1.el6_9

145280 - SuSE SLES 11 SP4 SUSE-SU-2017:0901-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8540, CVE-2016-10087

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0901-1

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-March/002778.html

SuSE SLES 11 SP4
i586
libpng12-0-1.2.31-5.43.1

x86_64
libpng12-0-1.2.31-5.43.1
libpng12-0-32bit-1.2.31-5.43.1

145281 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0860-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8540, CVE-2016-10087

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0860-1

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-March/002749.html

SuSE SLED 12 SP1
x86_64
libpng12-0-debuginfo-1.2.50-19.1
libpng12-0-debuginfo-32bit-1.2.50-19.1
libpng12-0-1.2.50-19.1
libpng12-0-32bit-1.2.50-19.1
libpng12-debugsource-1.2.50-19.1

SuSE SLES 12 SP2
x86_64
libpng12-0-debuginfo-1.2.50-19.1
libpng12-0-debuginfo-32bit-1.2.50-19.1
libpng12-0-1.2.50-19.1
libpng12-0-32bit-1.2.50-19.1
libpng12-debugsource-1.2.50-19.1

SuSE SLED 12 SP2
x86_64
libpng12-0-debuginfo-1.2.50-19.1
libpng12-0-debuginfo-32bit-1.2.50-19.1
libpng12-0-1.2.50-19.1
libpng12-0-32bit-1.2.50-19.1
libpng12-debugsource-1.2.50-19.1

SuSE SLES 12 SP1
x86_64
libpng12-0-debuginfo-1.2.50-19.1
libpng12-0-debuginfo-32bit-1.2.50-19.1
libpng12-0-1.2.50-19.1
libpng12-0-32bit-1.2.50-19.1
libpng12-debugsource-1.2.50-19.1

163319 - Oracle Enterprise Linux ELSA-2017-3533 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8952, CVE-2016-10088, CVE-2016-10147, CVE-2016-3140, CVE-2016-3672, CVE-2016-3951, CVE-2016-7097, CVE-2016-7425, CVE-2016-8399, CVE-2016-8632, CVE-2016-8633, CVE-2016-8645, CVE-2016-9178, CVE-2016-9588, CVE-2016-9644, CVE-2016-9756, CVE-2017-2596, CVE-2017-2636, CVE-2017-5897, CVE-2017-5970, CVE-2017-6001, CVE-2017-6345, CVE-2017-7187

Description

The scan detected that the host is missing the following update:
ELSA-2017-3533

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006816.html
http://oss.oracle.com/pipermail/el-errata/2017-April/006815.html

OEL7
x86_64
kernel-uek-4.1.12-61.1.33.el7uek
kernel-uek-debug-devel-4.1.12-61.1.33.el7uek
dtrace-modules-4.1.12-61.1.33.el7uek-0.5.3-2.el7
kernel-uek-devel-4.1.12-61.1.33.el7uek
kernel-uek-doc-4.1.12-61.1.33.el7uek
kernel-uek-debug-4.1.12-61.1.33.el7uek
kernel-uek-firmware-4.1.12-61.1.33.el7uek

OEL6
x86_64
kernel-uek-debug-devel-4.1.12-61.1.33.el6uek
kernel-uek-doc-4.1.12-61.1.33.el6uek
kernel-uek-devel-4.1.12-61.1.33.el6uek
kernel-uek-firmware-4.1.12-61.1.33.el6uek
kernel-uek-4.1.12-61.1.33.el6uek
dtrace-modules-4.1.12-61.1.33.el6uek-0.5.3-2.el6
kernel-uek-debug-4.1.12-61.1.33.el6uek

163321 - Oracle Enterprise Linux ELSA-2017-3534 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7446, CVE-2015-4700, CVE-2015-5707, CVE-2015-8569, CVE-2016-10088, CVE-2016-10142, CVE-2016-3140, CVE-2016-3672, CVE-2016-4482, CVE-2016-4485, CVE-2016-4580, CVE-2016-7425, CVE-2016-8399, CVE-2016-8633, CVE-2016-8645, CVE-2016-8646, CVE-2016-9178, CVE-2016-9588, CVE-2016-9644, CVE-2016-9793, CVE-2017-2636, CVE-2017-5970, CVE-2017-6074, CVE-2017-6345, CVE-2017-7187

Description

The scan detected that the host is missing the following update:
ELSA-2017-3534

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006818.html
http://oss.oracle.com/pipermail/el-errata/2017-April/006817.html

OEL7
x86_64
kernel-uek-doc-3.8.13-118.17.4.el7uek
kernel-uek-devel-3.8.13-118.17.4.el7uek
kernel-uek-debug-devel-3.8.13-118.17.4.el7uek
kernel-uek-debug-3.8.13-118.17.4.el7uek
kernel-uek-3.8.13-118.17.4.el7uek
kernel-uek-firmware-3.8.13-118.17.4.el7uek
dtrace-modules-3.8.13-118.17.4.el7uek-0.4.5-3.el7

OEL6
x86_64
kernel-uek-doc-3.8.13-118.17.4.el6uek
kernel-uek-debug-devel-3.8.13-118.17.4.el6uek
kernel-uek-devel-3.8.13-118.17.4.el6uek
dtrace-modules-3.8.13-118.17.4.el6uek-0.4.5-3.el6
kernel-uek-firmware-3.8.13-118.17.4.el6uek
kernel-uek-3.8.13-118.17.4.el6uek
kernel-uek-debug-3.8.13-118.17.4.el6uek

21534 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 45.8

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

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5409, CVE-2017-5410

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in several components. Successful exploitation could allow an attacker to bypass security access restrictions, retrieve sensitive data, remotely execute arbitrary code on the target system or cause a denial of service condition.

21535 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 45.8

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-5398, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5404, CVE-2017-5405, CVE-2017-5407, CVE-2017-5408, CVE-2017-5409, CVE-2017-5410

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in several components. Successful exploitation could allow an attacker to bypass security access restrictions, retrieve sensitive data, remotely execute arbitrary code on the target system or cause a denial of service condition.

21555 - Apple iTunes Multiple Vulnerabilities Prior To 12.6

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

Risk Level: High

CVE: CVE-2009-3270, CVE-2009-3560, CVE-2009-3720, CVE-2012-1147, CVE-2012-1148, CVE-2012-6702, CVE-2013-7443, CVE-2015-1283, CVE-2015-3414, CVE-2015-3415, CVE-2015-3416, CVE-2015-3717, CVE-2015-6607, CVE-2016-0718, CVE-2016-4472, CVE-2016-5300, CVE-2016-6153

Description

Multiple vulnerabilities are present in some versions of Apple iTunes.

Observation

Apple iTunes is a media management software.

Multiple vulnerabilities are present in some versions of Apple iTunes. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code, obtain sensitive information, cause a denial of service condition or possibly have other unspecified impact in the target system.

21556 - Apple iTunes Multiple Vulnerabilities Prior To 12.6

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2009-3270, CVE-2009-3560, CVE-2009-3720, CVE-2012-1147, CVE-2012-1148, CVE-2012-6702, CVE-2013-7443, CVE-2015-1283, CVE-2015-3414, CVE-2015-3415, CVE-2015-3416, CVE-2015-3717, CVE-2015-6607, CVE-2016-0718, CVE-2016-4472, CVE-2016-5300, CVE-2016-6153

Description

Multiple vulnerabilities are present in some versions of Apple iTunes.

Observation

Apple iTunes is a media management software.

Multiple vulnerabilities are present in some versions of Apple iTunes. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code, obtain sensitive information, cause a denial of service condition or possibly have other unspecified impact in the target system.

21560 - (K82508682) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-6074

Description

A vulnerability is present in some versions of F5 BIG-IP systems.

Observation

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

A vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the Linux kernel. Successful exploitation could allow an attacker to obtain elevated privileges or cause a denial-of-service.

21563 - Fatek Automation PLC Ethernet Module Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2017-6023

Description

A stack-based buffer overflow vulnerability is present in some versions of Fatek Ethernet Module Configure Tools.

Observation

Fatek Ethernet Module Configure Tools is created to aid the configuration of Ethernet module.

A stack-based buffer overflow vulnerability is present in some versions of Fatek Ethernet Module Configure Tools. This flaw lies in ether_cfg.exe. Successful exploitation could allow a remote attacker to crash the affected device or execute remote code.

21565 - Rockwell Automation Connected Components Workbench DLL Hijacking Vulnerability

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

Risk Level: High

CVE: CVE-2017-5176

Description

A DLL hijacking vulnerability is present in some versions of Rockwell Automation Connected Components Workbench.

Observation

Rockwell Automation Connected Components Workbench is a tool for controllers programming.

A DLL hijacking vulnerability is present in some versions of Rockwell Automation Connected Components Workbench. The flaw lies in how the product handle Dynamic-link Libraries. Successful exploitation could allow an attacker to cause a denial-of-service or execute arbitrary code.

21566 - (MFSA2017-08) Mozilla Firefox Integer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2017-5428

Description

An Integer overflow vulnerability is present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

An Integer overflow vulnerability is present in some versions of Mozilla Firefox. The flaw lies in createImageBitmap API. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system or cause a denial of service condition.

21567 - (MFSA2017-08) Mozilla Firefox Integer Overflow Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-5428

Description

An Integer overflow vulnerability is present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

An Integer overflow vulnerability is present in some versions of Mozilla Firefox. The flaw lies in createImageBitmap API. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system or cause a denial of service condition.

130737 - Debian Linux 8.0 DSA-3825-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3822

Description

The scan detected that the host is missing the following update:
DSA-3825-1

Observation

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

http://www.debian.org/security/2017/dsa-3825

Debian 8.0
all
jhead_1:2.97-1+deb8u1

132348 - Oracle VM OVMSA-2017-0055 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2857, CVE-2016-3710, CVE-2016-3712, CVE-2016-5403, CVE-2017-2615, CVE-2017-2620

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0055

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000664.html

OVM3.4
x86_64
qemu-img-0.12.1.2-2.503.el6

132349 - Oracle VM OVMSA-2017-0054 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5335, CVE-2017-5336, CVE-2017-5337

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0054

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000665.html
http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000671.html

OVM3.3
x86_64
gnutls-2.12.23-21.el6

OVM3.4
x86_64
gnutls-2.12.23-21.el6
gnutls-utils-2.12.23-21.el6

132350 - Oracle VM OVMSA-2017-0053 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8325

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0053

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000668.html
http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000663.html

OVM3.3
x86_64
openssh-server-5.3p1-122.el6
openssh-clients-5.3p1-122.el6
openssh-5.3p1-122.el6

OVM3.4

x86_64
openssh-server-5.3p1-122.el6
openssh-clients-5.3p1-122.el6
openssh-5.3p1-122.el6

132352 - Oracle VM OVMSA-2017-0051 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9761, CVE-2015-7547, CVE-2015-8776, CVE-2015-8778, CVE-2015-8779

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0051

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000661.html
http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000670.html

OVM3.3
x86_64
glibc-common-2.12-1.209.0.1.el6
glibc-2.12-1.209.0.1.el6
nscd-2.12-1.209.0.1.el6

OVM3.4
x86_64
glibc-headers-2.12-1.209.0.1.el6
glibc-common-2.12-1.209.0.1.el6
glibc-2.12-1.209.0.1.el6
glibc-devel-2.12-1.209.0.1.el6
nscd-2.12-1.209.0.1.el6

132355 - Oracle VM OVMSA-2017-0058 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4700, CVE-2015-5707, CVE-2016-10088, CVE-2016-10142, CVE-2016-3140, CVE-2016-3672, CVE-2016-4580, CVE-2016-7425, CVE-2016-8399, CVE-2016-8633, CVE-2016-8645, CVE-2017-2636, CVE-2017-6345, CVE-2017-7187

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0058

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-April/000676.html

OVM3.2
x86_64
kernel-uek-firmware-2.6.39-400.294.6.el5uek

kernel-uek-2.6.39-400.294.6.el5uek

141534 - Red Hat Enterprise Linux RHSA-2017-0869 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8399

Description

The scan detected that the host is missing the following update:
RHSA-2017-0869

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00004.html

RHEL6_7S
i386
kernel-devel-2.6.32-573.41.1.el6
kernel-debuginfo-common-i686-2.6.32-573.41.1.el6
python-perf-2.6.32-573.41.1.el6
perf-debuginfo-2.6.32-573.41.1.el6
perf-2.6.32-573.41.1.el6
kernel-debug-2.6.32-573.41.1.el6
kernel-debuginfo-2.6.32-573.41.1.el6
kernel-debug-debuginfo-2.6.32-573.41.1.el6
python-perf-debuginfo-2.6.32-573.41.1.el6
kernel-debug-devel-2.6.32-573.41.1.el6
kernel-headers-2.6.32-573.41.1.el6
kernel-2.6.32-573.41.1.el6

noarch
kernel-doc-2.6.32-573.41.1.el6
kernel-firmware-2.6.32-573.41.1.el6
kernel-abi-whitelists-2.6.32-573.41.1.el6

x86_64
kernel-debuginfo-common-x86_64-2.6.32-573.41.1.el6
kernel-2.6.32-573.41.1.el6
python-perf-debuginfo-2.6.32-573.41.1.el6
kernel-debug-2.6.32-573.41.1.el6
kernel-debug-debuginfo-2.6.32-573.41.1.el6
kernel-devel-2.6.32-573.41.1.el6
kernel-headers-2.6.32-573.41.1.el6
perf-2.6.32-573.41.1.el6
python-perf-2.6.32-573.41.1.el6
perf-debuginfo-2.6.32-573.41.1.el6
kernel-debuginfo-2.6.32-573.41.1.el6
kernel-debug-devel-2.6.32-573.41.1.el6
kernel-debuginfo-common-i686-2.6.32-573.41.1.el6

145279 - SuSE SLES 11 SP4 SUSE-SU-2017:0912-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0912-1

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-April/002779.html

SuSE SLES 11 SP4
i586
kernel-source-3.0.101-97.1
kernel-trace-devel-3.0.101-97.1
kernel-pae-devel-3.0.101-97.1
kernel-default-3.0.101-97.1
kernel-xen-devel-3.0.101-97.1
kernel-pae-base-3.0.101-97.1
kernel-trace-base-3.0.101-97.1
kernel-xen-base-3.0.101-97.1
kernel-pae-3.0.101-97.1
kernel-ec2-devel-3.0.101-97.1
kernel-ec2-base-3.0.101-97.1
kernel-trace-3.0.101-97.1
kernel-syms-3.0.101-97.1
kernel-ec2-3.0.101-97.1
kernel-default-base-3.0.101-97.1
kernel-default-devel-3.0.101-97.1
kernel-xen-3.0.101-97.1

x86_64
kernel-source-3.0.101-97.1
kernel-trace-devel-3.0.101-97.1
kernel-default-3.0.101-97.1
kernel-xen-devel-3.0.101-97.1
kernel-trace-base-3.0.101-97.1
kernel-xen-base-3.0.101-97.1
kernel-ec2-devel-3.0.101-97.1
kernel-ec2-base-3.0.101-97.1
kernel-trace-3.0.101-97.1
kernel-syms-3.0.101-97.1
kernel-ec2-3.0.101-97.1
kernel-default-base-3.0.101-97.1
kernel-default-devel-3.0.101-97.1
kernel-xen-3.0.101-97.1

145282 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:0858-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2619

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0858-1

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-March/002747.html

SuSE SLED 12 SP2
x86_64
libsamba-util0-debuginfo-4.4.2-36.2
samba-client-32bit-4.4.2-36.2
samba-debuginfo-4.4.2-36.2
libsmbconf0-debuginfo-32bit-4.4.2-36.2
libsmbclient0-4.4.2-36.2
libsamba-hostconfig0-32bit-4.4.2-36.2
libwbclient0-32bit-4.4.2-36.2
libnetapi0-debuginfo-4.4.2-36.2
libsamba-passdb0-debuginfo-32bit-4.4.2-36.2
samba-client-4.4.2-36.2
libdcerpc-binding0-debuginfo-32bit-4.4.2-36.2
libtevent-util0-32bit-4.4.2-36.2
libsamba-passdb0-4.4.2-36.2
libtevent-util0-4.4.2-36.2
libsamba-credentials0-4.4.2-36.2
libwbclient0-debuginfo-4.4.2-36.2
libsmbldap0-4.4.2-36.2
libsmbclient0-32bit-4.4.2-36.2
libtevent-util0-debuginfo-4.4.2-36.2
libsmbclient0-debuginfo-32bit-4.4.2-36.2
samba-winbind-4.4.2-36.2
samba-client-debuginfo-32bit-4.4.2-36.2
libdcerpc0-32bit-4.4.2-36.2
libdcerpc-binding0-debuginfo-4.4.2-36.2
libndr-nbt0-debuginfo-32bit-4.4.2-36.2
samba-winbind-32bit-4.4.2-36.2
libsmbldap0-32bit-4.4.2-36.2
libndr-nbt0-debuginfo-4.4.2-36.2
libdcerpc-binding0-32bit-4.4.2-36.2
libndr-standard0-debuginfo-4.4.2-36.2
libsmbconf0-debuginfo-4.4.2-36.2
libsamdb0-4.4.2-36.2
libdcerpc0-debuginfo-32bit-4.4.2-36.2
libsamba-credentials0-debuginfo-4.4.2-36.2
libsamba-util0-debuginfo-32bit-4.4.2-36.2
libndr-standard0-32bit-4.4.2-36.2
libsamba-passdb0-debuginfo-4.4.2-36.2
samba-debugsource-4.4.2-36.2
libsmbconf0-4.4.2-36.2
libnetapi0-4.4.2-36.2
libndr-krb5pac0-debuginfo-32bit-4.4.2-36.2
libwbclient0-4.4.2-36.2
libndr-nbt0-32bit-4.4.2-36.2
libndr0-4.4.2-36.2
libnetapi0-32bit-4.4.2-36.2
libsamba-passdb0-32bit-4.4.2-36.2
libtevent-util0-debuginfo-32bit-4.4.2-36.2
libsmbclient0-debuginfo-4.4.2-36.2
libndr-krb5pac0-debuginfo-4.4.2-36.2
samba-winbind-debuginfo-4.4.2-36.2
libsamba-util0-32bit-4.4.2-36.2
libdcerpc0-debuginfo-4.4.2-36.2

libndr-krb5pac0-32bit-4.4.2-36.2
libndr-krb5pac0-4.4.2-36.2
libsamba-util0-4.4.2-36.2
libsamba-hostconfig0-4.4.2-36.2
libsamdb0-32bit-4.4.2-36.2
libsmbldap0-debuginfo-32bit-4.4.2-36.2
libdcerpc0-4.4.2-36.2
libsamba-hostconfig0-debuginfo-32bit-4.4.2-36.2
samba-client-debuginfo-4.4.2-36.2
libndr0-32bit-4.4.2-36.2
samba-libs-32bit-4.4.2-36.2
libsamba-errors0-debuginfo-32bit-4.4.2-36.2
samba-libs-debuginfo-32bit-4.4.2-36.2
libdcerpc-binding0-4.4.2-36.2
libsamdb0-debuginfo-4.4.2-36.2
libsmbldap0-debuginfo-4.4.2-36.2
libsamba-errors0-4.4.2-36.2
samba-winbind-debuginfo-32bit-4.4.2-36.2
libsmbconf0-32bit-4.4.2-36.2
libwbclient0-debuginfo-32bit-4.4.2-36.2
samba-libs-4.4.2-36.2
libndr-standard0-debuginfo-32bit-4.4.2-36.2
libsamba-credentials0-debuginfo-32bit-4.4.2-36.2
libsamdb0-debuginfo-32bit-4.4.2-36.2
libsamba-credentials0-32bit-4.4.2-36.2
libsamba-hostconfig0-debuginfo-4.4.2-36.2
libsamba-errors0-32bit-4.4.2-36.2
samba-libs-debuginfo-4.4.2-36.2
libnetapi0-debuginfo-32bit-4.4.2-36.2
libndr0-debuginfo-4.4.2-36.2
libsamba-errors0-debuginfo-4.4.2-36.2
samba-4.4.2-36.2
libndr-standard0-4.4.2-36.2
libndr0-debuginfo-32bit-4.4.2-36.2
libndr-nbt0-4.4.2-36.2

noarch
samba-doc-4.4.2-36.2

SuSE SLES 12 SP2
noarch
samba-doc-4.4.2-36.2

x86_64
libsamba-util0-debuginfo-4.4.2-36.2
libtevent-util0-debuginfo-32bit-4.4.2-36.2
samba-client-32bit-4.4.2-36.2
libsmbldap0-debuginfo-4.4.2-36.2
libsmbconf0-debuginfo-32bit-4.4.2-36.2
libsmbclient0-4.4.2-36.2
libsmbclient0-debuginfo-4.4.2-36.2
libwbclient0-32bit-4.4.2-36.2
libnetapi0-debuginfo-4.4.2-36.2
libsamba-hostconfig0-32bit-4.4.2-36.2
samba-client-4.4.2-36.2
libdcerpc-binding0-debuginfo-32bit-4.4.2-36.2
libtevent-util0-32bit-4.4.2-36.2
libnetapi0-debuginfo-32bit-4.4.2-36.2
libtevent-util0-4.4.2-36.2
libsamdb0-4.4.2-36.2

samba-winbind-debuginfo-32bit-4.4.2-36.2
libsamba-passdb0-4.4.2-36.2
libsmbldap0-4.4.2-36.2
libsmbclient0-32bit-4.4.2-36.2
libtevent-util0-debuginfo-4.4.2-36.2
libsmbclient0-debuginfo-32bit-4.4.2-36.2
samba-client-debuginfo-32bit-4.4.2-36.2
libdcerpc0-32bit-4.4.2-36.2
libdcerpc-binding0-debuginfo-4.4.2-36.2
libsamba-passdb0-debuginfo-32bit-4.4.2-36.2
samba-winbind-32bit-4.4.2-36.2
libdcerpc0-debuginfo-32bit-4.4.2-36.2
libsmbldap0-32bit-4.4.2-36.2
libndr-nbt0-debuginfo-4.4.2-36.2
libdcerpc-binding0-32bit-4.4.2-36.2
libndr-standard0-debuginfo-4.4.2-36.2
libsmbconf0-debuginfo-4.4.2-36.2
samba-debuginfo-4.4.2-36.2
libsamba-credentials0-debuginfo-4.4.2-36.2
libsamba-util0-debuginfo-32bit-4.4.2-36.2
libndr-standard0-32bit-4.4.2-36.2
libsamba-passdb0-debuginfo-4.4.2-36.2
samba-debugsource-4.4.2-36.2
libsmbconf0-4.4.2-36.2
libnetapi0-4.4.2-36.2
libndr-krb5pac0-debuginfo-32bit-4.4.2-36.2
libwbclient0-4.4.2-36.2
libndr-nbt0-32bit-4.4.2-36.2
libndr0-4.4.2-36.2
libnetapi0-32bit-4.4.2-36.2
libsamba-passdb0-32bit-4.4.2-36.2
samba-winbind-debuginfo-4.4.2-36.2
libndr-krb5pac0-debuginfo-4.4.2-36.2
libndr-standard0-debuginfo-32bit-4.4.2-36.2
libsamba-util0-32bit-4.4.2-36.2
libdcerpc0-debuginfo-4.4.2-36.2
libsmbldap0-debuginfo-32bit-4.4.2-36.2
libndr-krb5pac0-32bit-4.4.2-36.2
libndr-krb5pac0-4.4.2-36.2
libsamdb0-32bit-4.4.2-36.2
libsamba-util0-4.4.2-36.2
libsamba-hostconfig0-4.4.2-36.2
samba-winbind-4.4.2-36.2
libwbclient0-debuginfo-4.4.2-36.2
libdcerpc0-4.4.2-36.2
libsamba-hostconfig0-debuginfo-32bit-4.4.2-36.2
samba-client-debuginfo-4.4.2-36.2
libndr0-32bit-4.4.2-36.2
samba-libs-32bit-4.4.2-36.2
libsamba-errors0-debuginfo-32bit-4.4.2-36.2
samba-libs-debuginfo-32bit-4.4.2-36.2
libdcerpc-binding0-4.4.2-36.2
libsamdb0-debuginfo-4.4.2-36.2
libndr-nbt0-debuginfo-32bit-4.4.2-36.2
libsamba-errors0-4.4.2-36.2
libsmbconf0-32bit-4.4.2-36.2
libwbclient0-debuginfo-32bit-4.4.2-36.2
samba-libs-4.4.2-36.2
libsamba-credentials0-4.4.2-36.2
libsamba-credentials0-debuginfo-32bit-4.4.2-36.2

libsamdb0-debuginfo-32bit-4.4.2-36.2
libsamba-credentials0-32bit-4.4.2-36.2
libsamba-hostconfig0-debuginfo-4.4.2-36.2
libsamba-errors0-32bit-4.4.2-36.2
samba-libs-debuginfo-4.4.2-36.2
libndr0-debuginfo-4.4.2-36.2
libsamba-errors0-debuginfo-4.4.2-36.2
samba-4.4.2-36.2
libndr-standard0-4.4.2-36.2
libndr0-debuginfo-32bit-4.4.2-36.2
libndr-nbt0-4.4.2-36.2

145283 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0859-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2619

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0859-1

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-March/002748.html

SuSE SLED 12 SP1
x86_64
libsamba-credentials0-debuginfo-4.2.4-28.8.2
libsmbldap0-debuginfo-4.2.4-28.8.2
libnetapi0-4.2.4-28.8.2
samba-client-debuginfo-32bit-4.2.4-28.8.2
libdcerpc-binding0-32bit-4.2.4-28.8.2
libsmbclient0-4.2.4-28.8.2
libwbclient0-debuginfo-4.2.4-28.8.2
libsamba-hostconfig0-4.2.4-28.8.2
libsmbclient0-debuginfo-4.2.4-28.8.2
libsamdb0-debuginfo-32bit-4.2.4-28.8.2
samba-libs-debuginfo-32bit-4.2.4-28.8.2
libtevent-util0-debuginfo-32bit-4.2.4-28.8.2
libndr-nbt0-4.2.4-28.8.2
libsmbclient-raw0-32bit-4.2.4-28.8.2
libsamba-credentials0-32bit-4.2.4-28.8.2
libsmbclient-raw0-debuginfo-32bit-4.2.4-28.8.2
samba-libs-debuginfo-4.2.4-28.8.2
libndr-krb5pac0-debuginfo-4.2.4-28.8.2
libsmbconf0-4.2.4-28.8.2
libgensec0-32bit-4.2.4-28.8.2
libndr-nbt0-debuginfo-4.2.4-28.8.2
libndr-krb5pac0-4.2.4-28.8.2
libndr0-debuginfo-32bit-4.2.4-28.8.2
libsamba-hostconfig0-debuginfo-4.2.4-28.8.2
samba-client-32bit-4.2.4-28.8.2
samba-debuginfo-4.2.4-28.8.2
samba-client-4.2.4-28.8.2
libtevent-util0-debuginfo-4.2.4-28.8.2

libgensec0-debuginfo-4.2.4-28.8.2
libndr0-4.2.4-28.8.2
libdcerpc-binding0-4.2.4-28.8.2
libsmbconf0-debuginfo-4.2.4-28.8.2
libsamba-util0-4.2.4-28.8.2
samba-libs-32bit-4.2.4-28.8.2
libsmbconf0-debuginfo-32bit-4.2.4-28.8.2
libsamba-credentials0-debuginfo-32bit-4.2.4-28.8.2
libndr-standard0-debuginfo-32bit-4.2.4-28.8.2
libndr-krb5pac0-32bit-4.2.4-28.8.2
libsmbldap0-debuginfo-32bit-4.2.4-28.8.2
libsamba-passdb0-debuginfo-32bit-4.2.4-28.8.2
samba-32bit-4.2.4-28.8.2
libndr-standard0-32bit-4.2.4-28.8.2
libnetapi0-debuginfo-4.2.4-28.8.2
libdcerpc0-32bit-4.2.4-28.8.2
samba-libs-4.2.4-28.8.2
libdcerpc0-4.2.4-28.8.2
libndr-nbt0-debuginfo-32bit-4.2.4-28.8.2
libsmbclient0-debuginfo-32bit-4.2.4-28.8.2
libdcerpc-binding0-debuginfo-32bit-4.2.4-28.8.2
libsamdb0-4.2.4-28.8.2
libsamba-credentials0-4.2.4-28.8.2
libndr-krb5pac0-debuginfo-32bit-4.2.4-28.8.2
samba-debugsource-4.2.4-28.8.2
libsamba-hostconfig0-32bit-4.2.4-28.8.2
libregistry0-debuginfo-4.2.4-28.8.2
libregistry0-4.2.4-28.8.2
libndr-standard0-debuginfo-4.2.4-28.8.2
samba-winbind-debuginfo-4.2.4-28.8.2
libsamba-passdb0-debuginfo-4.2.4-28.8.2
libsamba-util0-debuginfo-32bit-4.2.4-28.8.2
libdcerpc0-debuginfo-32bit-4.2.4-28.8.2
libdcerpc0-debuginfo-4.2.4-28.8.2
samba-4.2.4-28.8.2
samba-client-debuginfo-4.2.4-28.8.2
libsamba-util0-32bit-4.2.4-28.8.2
libwbclient0-32bit-4.2.4-28.8.2
libsmbldap0-32bit-4.2.4-28.8.2
libtevent-util0-4.2.4-28.8.2
libsmbclient0-32bit-4.2.4-28.8.2
libsamba-passdb0-4.2.4-28.8.2
libsamba-passdb0-32bit-4.2.4-28.8.2
libnetapi0-debuginfo-32bit-4.2.4-28.8.2
libndr-nbt0-32bit-4.2.4-28.8.2
libsamba-util0-debuginfo-4.2.4-28.8.2
libsamdb0-32bit-4.2.4-28.8.2
libgensec0-debuginfo-32bit-4.2.4-28.8.2
libtevent-util0-32bit-4.2.4-28.8.2
samba-debuginfo-32bit-4.2.4-28.8.2
libwbclient0-debuginfo-32bit-4.2.4-28.8.2
libdcerpc-binding0-debuginfo-4.2.4-28.8.2
libsmbclient-raw0-debuginfo-4.2.4-28.8.2
samba-winbind-debuginfo-32bit-4.2.4-28.8.2
libgensec0-4.2.4-28.8.2
libsmbldap0-4.2.4-28.8.2
libndr0-32bit-4.2.4-28.8.2
libsamdb0-debuginfo-4.2.4-28.8.2
libsamba-hostconfig0-debuginfo-32bit-4.2.4-28.8.2
libndr-standard0-4.2.4-28.8.2

libnetapi0-32bit-4.2.4-28.8.2
libsmbclient-raw0-4.2.4-28.8.2
libndr0-debuginfo-4.2.4-28.8.2
libsmbconf0-32bit-4.2.4-28.8.2
libwbclient0-4.2.4-28.8.2
samba-winbind-32bit-4.2.4-28.8.2
samba-winbind-4.2.4-28.8.2

noarch
samba-doc-4.2.4-28.8.2

SuSE SLES 12 SP2
x86_64
libdcerpc-atsvc0-debuginfo-4.2.4-28.8.2
libdcerpc-atsvc0-4.2.4-28.8.2

SuSE SLED 12 SP2
x86_64
libdcerpc-atsvc0-debuginfo-4.2.4-28.8.2
libdcerpc-atsvc0-4.2.4-28.8.2

SuSE SLES 12 SP1
noarch
samba-doc-4.2.4-28.8.2

x86_64
libsamba-credentials0-debuginfo-4.2.4-28.8.2
libsmbldap0-debuginfo-4.2.4-28.8.2
libnetapi0-4.2.4-28.8.2
samba-client-debuginfo-32bit-4.2.4-28.8.2
libdcerpc-binding0-32bit-4.2.4-28.8.2
libsmbclient0-4.2.4-28.8.2
libwbclient0-debuginfo-4.2.4-28.8.2
libsamba-hostconfig0-4.2.4-28.8.2
libsmbclient0-debuginfo-4.2.4-28.8.2
libsamdb0-debuginfo-32bit-4.2.4-28.8.2
samba-libs-debuginfo-32bit-4.2.4-28.8.2
libndr0-4.2.4-28.8.2
libsmbclient0-32bit-4.2.4-28.8.2
libndr-nbt0-4.2.4-28.8.2
libsmbclient-raw0-32bit-4.2.4-28.8.2
libsamba-credentials0-32bit-4.2.4-28.8.2
libsmbclient-raw0-debuginfo-32bit-4.2.4-28.8.2
samba-libs-debuginfo-4.2.4-28.8.2
libndr-krb5pac0-debuginfo-4.2.4-28.8.2
libgensec0-32bit-4.2.4-28.8.2
libndr-nbt0-debuginfo-4.2.4-28.8.2
libndr-krb5pac0-4.2.4-28.8.2
libsamba-util0-debuginfo-32bit-4.2.4-28.8.2
libndr0-debuginfo-32bit-4.2.4-28.8.2
libsamba-hostconfig0-debuginfo-4.2.4-28.8.2
samba-debugsource-4.2.4-28.8.2
samba-client-4.2.4-28.8.2
libgensec0-debuginfo-4.2.4-28.8.2
libsmbconf0-4.2.4-28.8.2
libdcerpc-binding0-4.2.4-28.8.2
libtevent-util0-32bit-4.2.4-28.8.2
libsamba-util0-4.2.4-28.8.2
samba-libs-32bit-4.2.4-28.8.2
libsamba-credentials0-debuginfo-32bit-4.2.4-28.8.2

libndr-standard0-debuginfo-32bit-4.2.4-28.8.2
libndr-krb5pac0-32bit-4.2.4-28.8.2
libsmbldap0-debuginfo-32bit-4.2.4-28.8.2
libsamba-passdb0-debuginfo-32bit-4.2.4-28.8.2
samba-32bit-4.2.4-28.8.2
libtevent-util0-debuginfo-4.2.4-28.8.2
libnetapi0-debuginfo-4.2.4-28.8.2
libdcerpc0-32bit-4.2.4-28.8.2
samba-libs-4.2.4-28.8.2
libdcerpc0-4.2.4-28.8.2
libndr-nbt0-debuginfo-32bit-4.2.4-28.8.2
libsmbclient0-debuginfo-32bit-4.2.4-28.8.2
libdcerpc-binding0-debuginfo-32bit-4.2.4-28.8.2
libsmbconf0-debuginfo-4.2.4-28.8.2
libsamba-credentials0-4.2.4-28.8.2
libndr-krb5pac0-debuginfo-32bit-4.2.4-28.8.2
libtevent-util0-debuginfo-32bit-4.2.4-28.8.2
libregistry0-debuginfo-4.2.4-28.8.2
libsamba-hostconfig0-32bit-4.2.4-28.8.2
libndr-standard0-debuginfo-4.2.4-28.8.2
libregistry0-4.2.4-28.8.2
samba-winbind-debuginfo-4.2.4-28.8.2
libsamba-passdb0-debuginfo-4.2.4-28.8.2
samba-debuginfo-4.2.4-28.8.2
libdcerpc0-debuginfo-32bit-4.2.4-28.8.2
libdcerpc0-debuginfo-4.2.4-28.8.2
samba-4.2.4-28.8.2
samba-client-debuginfo-4.2.4-28.8.2
libsamba-util0-debuginfo-4.2.4-28.8.2
libwbclient0-32bit-4.2.4-28.8.2
libsmbldap0-32bit-4.2.4-28.8.2
libtevent-util0-4.2.4-28.8.2
libsamba-passdb0-4.2.4-28.8.2
libsamdb0-4.2.4-28.8.2
libsamba-passdb0-32bit-4.2.4-28.8.2
libnetapi0-debuginfo-32bit-4.2.4-28.8.2
libndr-nbt0-32bit-4.2.4-28.8.2
libsmbconf0-debuginfo-32bit-4.2.4-28.8.2
libsamdb0-32bit-4.2.4-28.8.2
libgensec0-debuginfo-32bit-4.2.4-28.8.2
libwbclient0-4.2.4-28.8.2
samba-debuginfo-32bit-4.2.4-28.8.2
libwbclient0-debuginfo-32bit-4.2.4-28.8.2
libdcerpc-binding0-debuginfo-4.2.4-28.8.2
samba-client-32bit-4.2.4-28.8.2
libsmbclient-raw0-debuginfo-4.2.4-28.8.2
samba-winbind-debuginfo-32bit-4.2.4-28.8.2
libgensec0-4.2.4-28.8.2
libsmbldap0-4.2.4-28.8.2
libsamba-util0-32bit-4.2.4-28.8.2
libndr0-32bit-4.2.4-28.8.2
libsamdb0-debuginfo-4.2.4-28.8.2
libsamba-hostconfig0-debuginfo-32bit-4.2.4-28.8.2
libndr-standard0-4.2.4-28.8.2
libnetapi0-32bit-4.2.4-28.8.2
libsmbclient-raw0-4.2.4-28.8.2
libndr0-debuginfo-4.2.4-28.8.2
libsmbconf0-32bit-4.2.4-28.8.2

145284 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:0864-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636, CVE-2017-7184

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0864-1

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-March/002751.html

SuSE SLED 12 SP2
x86_64
kernel-default-4.4.49-92.14.1
kernel-default-devel-4.4.49-92.14.1
kernel-default-debugsource-4.4.49-92.14.1
kernel-default-debuginfo-4.4.49-92.14.1
kernel-default-extra-4.4.49-92.14.1
kernel-syms-4.4.49-92.14.1
kernel-default-extra-debuginfo-4.4.49-92.14.1

noarch
kernel-source-4.4.49-92.14.1
kernel-macros-4.4.49-92.14.1
kernel-devel-4.4.49-92.14.1

SuSE SLES 12 SP2
noarch
kernel-source-4.4.49-92.14.1
kernel-macros-4.4.49-92.14.1
kernel-devel-4.4.49-92.14.1

x86_64
kernel-default-4.4.49-92.14.1
kernel-default-devel-4.4.49-92.14.1
kernel-default-debugsource-4.4.49-92.14.1
kernel-default-debuginfo-4.4.49-92.14.1
kernel-default-base-4.4.49-92.14.1
kernel-default-base-debuginfo-4.4.49-92.14.1
kernel-syms-4.4.49-92.14.1

145285 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2017:0865-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2636, CVE-2017-7184

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0865-1

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-March/002752.html

SuSE SLES 12 SP1
noarch
kernel-source-3.12.69-60.64.35.1
kernel-devel-3.12.69-60.64.35.1
kernel-macros-3.12.69-60.64.35.1

x86_64
kernel-syms-3.12.69-60.64.35.1
kernel-xen-3.12.69-60.64.35.1
kernel-default-base-3.12.69-60.64.35.1
kernel-xen-debugsource-3.12.69-60.64.35.1
kernel-default-base-debuginfo-3.12.69-60.64.35.1
kernel-default-debuginfo-3.12.69-60.64.35.1
kernel-xen-base-3.12.69-60.64.35.1
kernel-xen-debuginfo-3.12.69-60.64.35.1
kernel-default-3.12.69-60.64.35.1
kernel-default-devel-3.12.69-60.64.35.1
kernel-default-debugsource-3.12.69-60.64.35.1
kernel-xen-base-debuginfo-3.12.69-60.64.35.1
kernel-xen-devel-3.12.69-60.64.35.1

SuSE SLED 12 SP1
x86_64
kernel-xen-devel-3.12.69-60.64.35.1
kernel-default-extra-3.12.69-60.64.35.1
kernel-default-debugsource-3.12.69-60.64.35.1
kernel-default-3.12.69-60.64.35.1
kernel-xen-debugsource-3.12.69-60.64.35.1
kernel-default-extra-debuginfo-3.12.69-60.64.35.1
kernel-xen-debuginfo-3.12.69-60.64.35.1
kernel-xen-3.12.69-60.64.35.1
kernel-syms-3.12.69-60.64.35.1
kernel-default-devel-3.12.69-60.64.35.1
kernel-default-debuginfo-3.12.69-60.64.35.1

noarch
kernel-source-3.12.69-60.64.35.1
kernel-devel-3.12.69-60.64.35.1
kernel-macros-3.12.69-60.64.35.1

163320 - Oracle Enterprise Linux ELSA-2017-3535 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4700, CVE-2015-5707, CVE-2016-10088, CVE-2016-10142, CVE-2016-3140, CVE-2016-3672, CVE-2016-4580, CVE-2016-7425, CVE-2016-8399, CVE-2016-8633, CVE-2016-8645, CVE-2017-2636, CVE-2017-6345, CVE-2017-7187

Description

The scan detected that the host is missing the following update:
ELSA-2017-3535

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-April/006820.html
http://oss.oracle.com/pipermail/el-errata/2017-April/006819.html

OEL5
x86_64
kernel-uek-doc-2.6.39-400.294.6.el5uek
kernel-uek-firmware-2.6.39-400.294.6.el5uek
kernel-uek-debug-2.6.39-400.294.6.el5uek
kernel-uek-debug-devel-2.6.39-400.294.6.el5uek
kernel-uek-2.6.39-400.294.6.el5uek
kernel-uek-devel-2.6.39-400.294.6.el5uek

i386
kernel-uek-doc-2.6.39-400.294.6.el5uek
kernel-uek-debug-2.6.39-400.294.6.el5uek
kernel-uek-firmware-2.6.39-400.294.6.el5uek
kernel-uek-debug-devel-2.6.39-400.294.6.el5uek
kernel-uek-2.6.39-400.294.6.el5uek
kernel-uek-devel-2.6.39-400.294.6.el5uek

OEL6
x86_64
kernel-uek-firmware-2.6.39-400.294.6.el6uek
kernel-uek-debug-devel-2.6.39-400.294.6.el6uek
kernel-uek-doc-2.6.39-400.294.6.el6uek
kernel-uek-2.6.39-400.294.6.el6uek
kernel-uek-debug-2.6.39-400.294.6.el6uek
kernel-uek-devel-2.6.39-400.294.6.el6uek

i386
kernel-uek-firmware-2.6.39-400.294.6.el6uek
kernel-uek-debug-devel-2.6.39-400.294.6.el6uek
kernel-uek-doc-2.6.39-400.294.6.el6uek
kernel-uek-2.6.39-400.294.6.el6uek
kernel-uek-debug-2.6.39-400.294.6.el6uek
kernel-uek-devel-2.6.39-400.294.6.el6uek

170785 - Amazon Linux AMI ALAS-2017-808 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-10158, CVE-2016-10159, CVE-2016-10160, CVE-2016-10161, CVE-2016-10167, CVE-2016-10168

Description

The scan detected that the host is missing the following update:
ALAS-2017-808

Observation

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

https://alas.aws.amazon.com/ALAS-2017-808.html

Amazon Linux AMI
x86_64
php56-gd-5.6.30-1.133.amzn1
php56-pgsql-5.6.30-1.133.amzn1
php56-embedded-5.6.30-1.133.amzn1

php56-debuginfo-5.6.30-1.133.amzn1
php56-snmp-5.6.30-1.133.amzn1
php56-mysqlnd-5.6.30-1.133.amzn1
php56-mssql-5.6.30-1.133.amzn1
php56-intl-5.6.30-1.133.amzn1
php56-pspell-5.6.30-1.133.amzn1
php56-opcache-5.6.30-1.133.amzn1
php56-fpm-5.6.30-1.133.amzn1
php56-mbstring-5.6.30-1.133.amzn1
php56-bcmath-5.6.30-1.133.amzn1
php56-imap-5.6.30-1.133.amzn1
php56-xml-5.6.30-1.133.amzn1
php56-recode-5.6.30-1.133.amzn1
php56-5.6.30-1.133.amzn1
php56-cli-5.6.30-1.133.amzn1
php56-pdo-5.6.30-1.133.amzn1
php56-common-5.6.30-1.133.amzn1
php56-mcrypt-5.6.30-1.133.amzn1
php56-dbg-5.6.30-1.133.amzn1
php56-soap-5.6.30-1.133.amzn1
php56-ldap-5.6.30-1.133.amzn1
php56-process-5.6.30-1.133.amzn1
php56-dba-5.6.30-1.133.amzn1
php56-odbc-5.6.30-1.133.amzn1
php56-tidy-5.6.30-1.133.amzn1
php56-enchant-5.6.30-1.133.amzn1
php56-devel-5.6.30-1.133.amzn1
php56-xmlrpc-5.6.30-1.133.amzn1
php56-gmp-5.6.30-1.133.amzn1

i686
php56-gd-5.6.30-1.133.amzn1
php56-pgsql-5.6.30-1.133.amzn1
php56-embedded-5.6.30-1.133.amzn1
php56-debuginfo-5.6.30-1.133.amzn1
php56-snmp-5.6.30-1.133.amzn1
php56-mysqlnd-5.6.30-1.133.amzn1
php56-mssql-5.6.30-1.133.amzn1
php56-intl-5.6.30-1.133.amzn1
php56-mbstring-5.6.30-1.133.amzn1
php56-opcache-5.6.30-1.133.amzn1
php56-fpm-5.6.30-1.133.amzn1
php56-recode-5.6.30-1.133.amzn1
php56-bcmath-5.6.30-1.133.amzn1
php56-imap-5.6.30-1.133.amzn1
php56-xml-5.6.30-1.133.amzn1
php56-pspell-5.6.30-1.133.amzn1
php56-5.6.30-1.133.amzn1
php56-cli-5.6.30-1.133.amzn1
php56-pdo-5.6.30-1.133.amzn1
php56-common-5.6.30-1.133.amzn1
php56-mcrypt-5.6.30-1.133.amzn1
php56-dbg-5.6.30-1.133.amzn1
php56-soap-5.6.30-1.133.amzn1
php56-ldap-5.6.30-1.133.amzn1
php56-process-5.6.30-1.133.amzn1
php56-dba-5.6.30-1.133.amzn1
php56-odbc-5.6.30-1.133.amzn1
php56-tidy-5.6.30-1.133.amzn1
php56-enchant-5.6.30-1.133.amzn1

php56-devel-5.6.30-1.133.amzn1
php56-xmlrpc-5.6.30-1.133.amzn1
php56-gmp-5.6.30-1.133.amzn1

170786 - Amazon Linux AMI ALAS-2017-809 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-5953, CVE-2017-6349, CVE-2017-6350

Description

The scan detected that the host is missing the following update:
ALAS-2017-809

Observation

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

https://alas.aws.amazon.com/ALAS-2017-809.html

Amazon Linux AMI
x86_64
vim-debuginfo-8.0.0503-1.45.amzn1
vim-enhanced-8.0.0503-1.45.amzn1
vim-filesystem-8.0.0503-1.45.amzn1
vim-common-8.0.0503-1.45.amzn1
vim-minimal-8.0.0503-1.45.amzn1

i686
vim-debuginfo-8.0.0503-1.45.amzn1
vim-enhanced-8.0.0503-1.45.amzn1
vim-filesystem-8.0.0503-1.45.amzn1
vim-common-8.0.0503-1.45.amzn1
vim-minimal-8.0.0503-1.45.amzn1

170788 - Amazon Linux AMI ALAS-2017-811 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-6347, CVE-2017-7184

Description

The scan detected that the host is missing the following update:
ALAS-2017-811

Observation

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

https://alas.aws.amazon.com/ALAS-2017-811.html

Amazon Linux AMI
i686
kernel-tools-debuginfo-4.4.51-40.60.amzn1
perf-4.4.51-40.60.amzn1
kernel-headers-4.4.51-40.60.amzn1

kernel-devel-4.4.51-40.60.amzn1
perf-debuginfo-4.4.51-40.60.amzn1
kernel-tools-4.4.51-40.60.amzn1
kernel-debuginfo-4.4.51-40.60.amzn1
kernel-debuginfo-common-i686-4.4.51-40.60.amzn1
kernel-4.4.51-40.60.amzn1
kernel-tools-devel-4.4.51-40.60.amzn1

noarch
kernel-doc-4.4.51-40.60.amzn1

x86_64
perf-4.4.51-40.60.amzn1
kernel-tools-debuginfo-4.4.51-40.60.amzn1
kernel-tools-4.4.51-40.60.amzn1
kernel-headers-4.4.51-40.60.amzn1
kernel-devel-4.4.51-40.60.amzn1
kernel-debuginfo-common-x86_64-4.4.51-40.60.amzn1
perf-debuginfo-4.4.51-40.60.amzn1
kernel-debuginfo-4.4.51-40.60.amzn1
kernel-4.4.51-40.60.amzn1
kernel-tools-devel-4.4.51-40.60.amzn1

170789 - Amazon Linux AMI ALAS-2017-812 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-10158, CVE-2016-10159, CVE-2016-10160, CVE-2016-10161, CVE-2016-10162, CVE-2016-10167, CVE-2016-10168, CVE-2016-7479, CVE-2017-5340

Description

The scan detected that the host is missing the following update:
ALAS-2017-812

Observation

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

https://alas.aws.amazon.com/ALAS-2017-812.html

Amazon Linux AMI
x86_64
php70-devel-7.0.16-1.21.amzn1
php70-gmp-7.0.16-1.21.amzn1
php70-mbstring-7.0.16-1.21.amzn1
php70-dba-7.0.16-1.21.amzn1
php70-enchant-7.0.16-1.21.amzn1
php70-embedded-7.0.16-1.21.amzn1
php70-pspell-7.0.16-1.21.amzn1
php70-json-7.0.16-1.21.amzn1
php70-fpm-7.0.16-1.21.amzn1
php70-recode-7.0.16-1.21.amzn1
php70-intl-7.0.16-1.21.amzn1
php70-tidy-7.0.16-1.21.amzn1
php70-mcrypt-7.0.16-1.21.amzn1
php70-gd-7.0.16-1.21.amzn1
php70-process-7.0.16-1.21.amzn1
php70-mysqlnd-7.0.16-1.21.amzn1

php70-imap-7.0.16-1.21.amzn1
php70-pgsql-7.0.16-1.21.amzn1
php70-zip-7.0.16-1.21.amzn1
php70-debuginfo-7.0.16-1.21.amzn1
php70-7.0.16-1.21.amzn1
php70-pdo-7.0.16-1.21.amzn1
php70-bcmath-7.0.16-1.21.amzn1
php70-soap-7.0.16-1.21.amzn1
php70-dbg-7.0.16-1.21.amzn1
php70-odbc-7.0.16-1.21.amzn1
php70-cli-7.0.16-1.21.amzn1
php70-xml-7.0.16-1.21.amzn1
php70-common-7.0.16-1.21.amzn1
php70-pdo-dblib-7.0.16-1.21.amzn1
php70-xmlrpc-7.0.16-1.21.amzn1
php70-opcache-7.0.16-1.21.amzn1
php70-snmp-7.0.16-1.21.amzn1
php70-ldap-7.0.16-1.21.amzn1

i686
php70-devel-7.0.16-1.21.amzn1
php70-bcmath-7.0.16-1.21.amzn1
php70-gmp-7.0.16-1.21.amzn1
php70-pdo-7.0.16-1.21.amzn1
php70-dba-7.0.16-1.21.amzn1
php70-enchant-7.0.16-1.21.amzn1
php70-embedded-7.0.16-1.21.amzn1
php70-pspell-7.0.16-1.21.amzn1
php70-json-7.0.16-1.21.amzn1
php70-fpm-7.0.16-1.21.amzn1
php70-recode-7.0.16-1.21.amzn1
php70-intl-7.0.16-1.21.amzn1
php70-tidy-7.0.16-1.21.amzn1
php70-mcrypt-7.0.16-1.21.amzn1
php70-gd-7.0.16-1.21.amzn1
php70-process-7.0.16-1.21.amzn1
php70-mysqlnd-7.0.16-1.21.amzn1
php70-imap-7.0.16-1.21.amzn1
php70-pgsql-7.0.16-1.21.amzn1
php70-zip-7.0.16-1.21.amzn1
php70-debuginfo-7.0.16-1.21.amzn1
php70-7.0.16-1.21.amzn1
php70-cli-7.0.16-1.21.amzn1
php70-soap-7.0.16-1.21.amzn1
php70-dbg-7.0.16-1.21.amzn1
php70-odbc-7.0.16-1.21.amzn1
php70-pdo-dblib-7.0.16-1.21.amzn1
php70-xml-7.0.16-1.21.amzn1
php70-common-7.0.16-1.21.amzn1
php70-xmlrpc-7.0.16-1.21.amzn1
php70-opcache-7.0.16-1.21.amzn1
php70-snmp-7.0.16-1.21.amzn1
php70-mbstring-7.0.16-1.21.amzn1
php70-ldap-7.0.16-1.21.amzn1

170790 - Amazon Linux AMI ALAS-2017-813 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-4075, CVE-2015-3811, CVE-2015-3812, CVE-2015-3813

Description

The scan detected that the host is missing the following update:
ALAS-2017-813

Observation

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

https://alas.aws.amazon.com/ALAS-2017-813.html

Amazon Linux AMI
x86_64
wireshark-1.8.10-25.22.amzn1
wireshark-devel-1.8.10-25.22.amzn1
wireshark-debuginfo-1.8.10-25.22.amzn1

i686
wireshark-1.8.10-25.22.amzn1
wireshark-devel-1.8.10-25.22.amzn1
wireshark-debuginfo-1.8.10-25.22.amzn1

182321 - FreeBSD NVIDIA UNIX driver Multiple Vulnerabilities In The Kernel Mode Layer Handler (057e6616-1885-11e7-bb4d-a0d3c19bfa21)

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

Risk Level: High

CVE: CVE-2017-0309, CVE-2017-0310, CVE-2017-0311, CVE-2017-0318, CVE-2017-0321

Description

The scan detected that the host is missing the following update:
NVIDIA UNIX driver -- multiple vulnerabilities in the kernel mode layer handler (057e6616-1885-11e7-bb4d-a0d3c19bfa21)

Observation

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

http://www.vuxml.org/freebsd/057e6616-1885-11e7-bb4d-a0d3c19bfa21.html

Affected packages:
nvidia-driver < 375.39
nvidia-driver-340 < 340.102
nvidia-driver-304 < 304.135

185647 - Ubuntu Linux 12.04 USN-3250-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7184

Description

The scan detected that the host is missing the following update:
USN-3250-2

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-March/003802.html

Ubuntu 12.04

linux-image-generic-lpae-lts-trusty_3.13.0.115.106
linux-image-generic-lts-trusty_3.13.0.115.106
linux-image-3.13.0-115-generic_3.13.0-115.162~precise1
linux-image-3.13.0-115-generic-lpae_3.13.0-115.162~precise1

185648 - Ubuntu Linux 12.04, 14.04, 16.04 USN-3256-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7308

Description

The scan detected that the host is missing the following update:
USN-3256-2

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-April/003811.html

Ubuntu 12.04

linux-image-generic-lpae-lts-trusty_3.13.0.116.107
linux-image-generic-lts-trusty_3.13.0.116.107
linux-image-3.13.0-116-generic_3.13.0-116.163~precise1
linux-image-3.13.0-116-generic-lpae_3.13.0-116.163~precise1

Ubuntu 16.04

linux-image-generic-hwe-16.04_4.8.0.46.18
linux-image-lowlatency-hwe-16.04_4.8.0.46.18
linux-image-4.8.0-46-generic-lpae_4.8.0-46.49~16.04.1
linux-image-4.8.0-46-lowlatency_4.8.0-46.49~16.04.1
linux-image-4.8.0-46-generic_4.8.0-46.49~16.04.1
linux-image-generic-lpae-hwe-16.04_4.8.0.46.18

Ubuntu 14.04

linux-image-powerpc-smp-lts-xenial_4.4.0.72.59
linux-image-powerpc64-smp-lts-xenial_4.4.0.72.59
linux-image-4.4.0-72-powerpc-smp_4.4.0-72.93~14.04.1
linux-image-generic-lpae-lts-xenial_4.4.0.72.59
linux-image-lowlatency-lts-xenial_4.4.0.72.59
linux-image-4.4.0-72-lowlatency_4.4.0-72.93~14.04.1
linux-image-4.4.0-72-powerpc-e500mc_4.4.0-72.93~14.04.1
linux-image-4.4.0-72-powerpc64-smp_4.4.0-72.93~14.04.1
linux-image-generic-lts-xenial_4.4.0.72.59
linux-image-4.4.0-72-generic_4.4.0-72.93~14.04.1
linux-image-powerpc-e500mc-lts-xenial_4.4.0.72.59

linux-image-4.4.0-72-generic-lpae_4.4.0-72.93~14.04.1

185649 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3256-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7308

Description

The scan detected that the host is missing the following update:
USN-3256-1

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-April/003810.html

Ubuntu 12.04

linux-image-3.2.0-126-omap_3.2.0-126.169
linux-image-3.2.0-1504-omap4_3.2.0-1504.131
linux-image-3.2.0-126-powerpc-smp_3.2.0-126.169
linux-image-3.2.0-126-powerpc64-smp_3.2.0-126.169
linux-image-3.2.0-126-generic-pae_3.2.0-126.169
linux-image-powerpc64-smp_3.2.0.126.141
linux-image-3.2.0-126-virtual_3.2.0-126.169
linux-image-omap4_3.2.0.1504.99
linux-image-generic-pae_3.2.0.126.141
linux-image-virtual_3.2.0.126.141
linux-image-3.2.0-126-highbank_3.2.0-126.169
linux-image-generic_3.2.0.126.141
linux-image-highbank_3.2.0.126.141
linux-image-omap_3.2.0.126.141
linux-image-3.2.0-126-generic_3.2.0-126.169
linux-image-powerpc-smp_3.2.0.126.141

Ubuntu 16.04

linux-image-snapdragon_4.4.0.1055.48
linux-image-powerpc-e500mc_4.4.0.72.78
linux-image-powerpc64-smp-lts-utopic_4.4.0.72.78
linux-image-4.4.0-72-lowlatency_4.4.0-72.93
linux-image-powerpc64-smp_4.4.0.72.78
linux-image-4.4.0-72-generic_4.4.0-72.93
linux-image-powerpc64-smp-lts-xenial_4.4.0.72.78
linux-image-4.4.0-1013-aws_4.4.0-1013.22
linux-image-generic-lpae_4.4.0.72.78
linux-image-4.4.0-1052-raspi2_4.4.0-1052.59
linux-image-4.4.0-72-powerpc-smp_4.4.0-72.93
linux-image-lowlatency_4.4.0.72.78
linux-image-4.4.0-72-powerpc-e500mc_4.4.0-72.93
linux-image-powerpc64-smp-lts-wily_4.4.0.72.78
linux-image-gke_4.4.0.1010.12
linux-image-powerpc-smp_4.4.0.72.78
linux-image-4.4.0-72-generic-lpae_4.4.0-72.93
linux-image-4.4.0-1055-snapdragon_4.4.0-1055.59
linux-image-raspi2_4.4.0.1052.53

linux-image-4.4.0-1010-gke_4.4.0-1010.10
linux-image-4.4.0-72-powerpc64-smp_4.4.0-72.93
linux-image-powerpc64-smp-lts-vivid_4.4.0.72.78
linux-image-aws_4.4.0.1013.16
linux-image-generic_4.4.0.72.78

Ubuntu 14.04

linux-image-powerpc64-smp_3.13.0.116.126
linux-image-3.13.0-116-powerpc-e500_3.13.0-116.163
linux-image-powerpc-e500_3.13.0.116.126
linux-image-3.13.0-116-generic-lpae_3.13.0-116.163
linux-image-3.13.0-116-powerpc-smp_3.13.0-116.163
linux-image-3.13.0-116-generic_3.13.0-116.163
linux-image-powerpc-e500mc_3.13.0.116.126
linux-image-lowlatency_3.13.0.116.126
linux-image-3.13.0-116-powerpc64-smp_3.13.0-116.163
linux-image-generic_3.13.0.116.126
linux-image-3.13.0-116-lowlatency_3.13.0-116.163
linux-image-generic-lpae_3.13.0.116.126
linux-image-powerpc-smp_3.13.0.116.126
linux-image-3.13.0-116-powerpc-e500mc_3.13.0-116.163

Ubuntu 16.10

linux-image-powerpc64-smp_4.8.0.46.58
linux-image-4.8.0-46-powerpc-smp_4.8.0-46.49
linux-image-lowlatency_4.8.0.46.58
linux-image-4.8.0-46-generic_4.8.0-46.49
linux-image-4.8.0-46-powerpc-e500mc_4.8.0-46.49
linux-image-4.8.0-46-powerpc64-emb_4.8.0-46.49
linux-image-4.8.0-46-lowlatency_4.8.0-46.49
linux-image-generic-lpae_4.8.0.46.58
linux-image-powerpc-e500mc_4.8.0.46.58
linux-image-powerpc-smp_4.8.0.46.58
linux-image-raspi2_4.8.0.1033.37
linux-image-4.8.0-46-generic-lpae_4.8.0-46.49
linux-image-4.8.0-1033-raspi2_4.8.0-1033.36
linux-image-generic_4.8.0.46.58

185651 - Ubuntu Linux 16.04 USN-3251-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7184

Description

The scan detected that the host is missing the following update:
USN-3251-2

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-March/003804.html

Ubuntu 16.04

linux-image-generic-lpae-hwe-16.04_4.8.0.45.17
linux-image-4.8.0-45-generic-lpae_4.8.0-45.48~16.04.1
linux-image-4.8.0-45-generic_4.8.0-45.48~16.04.1
linux-image-lowlatency-hwe-16.04_4.8.0.45.17
linux-image-4.8.0-45-lowlatency_4.8.0-45.48~16.04.1
linux-image-generic-hwe-16.04_4.8.0.45.17

185653 - Ubuntu Linux 14.04 USN-3249-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7184

Description

The scan detected that the host is missing the following update:
USN-3249-2

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-March/003800.html

Ubuntu 14.04

linux-image-4.4.0-71-lowlatency_4.4.0-71.92~14.04.1
linux-image-generic-lpae-lts-xenial_4.4.0.71.58
linux-image-lowlatency-lts-xenial_4.4.0.71.58
linux-image-powerpc-e500mc-lts-xenial_4.4.0.71.58
linux-image-powerpc-smp-lts-xenial_4.4.0.71.58
linux-image-4.4.0-71-powerpc64-smp_4.4.0-71.92~14.04.1
linux-image-4.4.0-71-powerpc-smp_4.4.0-71.92~14.04.1
linux-image-4.4.0-71-powerpc-e500mc_4.4.0-71.92~14.04.1
linux-image-4.4.0-71-generic-lpae_4.4.0-71.92~14.04.1
linux-image-powerpc64-smp-lts-xenial_4.4.0.71.58
linux-image-generic-lts-xenial_4.4.0.71.58
linux-image-4.4.0-71-generic_4.4.0-71.92~14.04.1

185654 - Ubuntu Linux 16.10 USN-3251-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7184

Description

The scan detected that the host is missing the following update:
USN-3251-1

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-March/003803.html

Ubuntu 16.10

linux-image-powerpc-e500mc_4.8.0.45.57
linux-image-generic_4.8.0.45.57
linux-image-4.8.0-45-generic_4.8.0-45.48
linux-image-powerpc-smp_4.8.0.45.57
linux-image-4.8.0-45-powerpc-smp_4.8.0-45.48
linux-image-4.8.0-45-generic-lpae_4.8.0-45.48
linux-image-lowlatency_4.8.0.45.57
linux-image-generic-lpae_4.8.0.45.57
linux-image-raspi2_4.8.0.1032.36
linux-image-4.8.0-45-lowlatency_4.8.0-45.48
linux-image-4.8.0-1032-raspi2_4.8.0-1032.35
linux-image-4.8.0-45-powerpc-e500mc_4.8.0-45.48

185655 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3253-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-7108, CVE-2013-7205, CVE-2014-1878, CVE-2016-9566

Description

The scan detected that the host is missing the following update:
USN-3253-1

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-April/003807.html

Ubuntu 16.04

nagios3-core_3.5.1.dfsg-2.1ubuntu1.1
nagios3-cgi_3.5.1.dfsg-2.1ubuntu1.1

Ubuntu 14.04

nagios3-cgi_3.5.1-1ubuntu1.1
nagios3-core_3.5.1-1ubuntu1.1

Ubuntu 16.10

nagios3-core_3.5.1.dfsg-2.1ubuntu3.1
nagios3-cgi_3.5.1.dfsg-2.1ubuntu3.1

185656 - Ubuntu Linux 12.04 USN-3248-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7184

Description

The scan detected that the host is missing the following update:
USN-3248-1

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-March/003798.html

Ubuntu 12.04

linux-image-3.2.0-125-generic-pae_3.2.0-125.168
linux-image-3.2.0-125-powerpc64-smp_3.2.0-125.168
linux-image-3.2.0-125-generic_3.2.0-125.168
linux-image-powerpc64-smp_3.2.0.125.140
linux-image-3.2.0-125-omap_3.2.0-125.168
linux-image-omap4_3.2.0.1503.98
linux-image-3.2.0-1503-omap4_3.2.0-1503.130
linux-image-generic_3.2.0.125.140
linux-image-virtual_3.2.0.125.140
linux-image-3.2.0-125-virtual_3.2.0-125.168
linux-image-powerpc-smp_3.2.0.125.140
linux-image-generic-pae_3.2.0.125.140
linux-image-3.2.0-125-powerpc-smp_3.2.0-125.168
linux-image-omap_3.2.0.125.140
linux-image-3.2.0-125-highbank_3.2.0-125.168
linux-image-highbank_3.2.0.125.140

185659 - Ubuntu Linux 14.04 USN-3250-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7184

Description

The scan detected that the host is missing the following update:
USN-3250-1

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-March/003801.html

Ubuntu 14.04

linux-image-3.13.0-115-generic-lpae_3.13.0-115.162
linux-image-generic-lpae_3.13.0.115.125
linux-image-3.13.0-115-powerpc-smp_3.13.0-115.162
linux-image-powerpc-smp_3.13.0.115.125
linux-image-powerpc64-smp_3.13.0.115.125
linux-image-powerpc-e500mc_3.13.0.115.125
linux-image-3.13.0-115-powerpc64-smp_3.13.0-115.162
linux-image-3.13.0-115-powerpc-e500mc_3.13.0-115.162
linux-image-3.13.0-115-powerpc-e500_3.13.0-115.162
linux-image-generic_3.13.0.115.125
linux-image-3.13.0-115-generic_3.13.0-115.162
linux-image-powerpc-e500_3.13.0.115.125
linux-image-3.13.0-115-lowlatency_3.13.0-115.162
linux-image-lowlatency_3.13.0.115.125

185660 - Ubuntu Linux 16.04 USN-3249-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7184

Description

The scan detected that the host is missing the following update:
USN-3249-1

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-March/003799.html

Ubuntu 16.04

linux-image-gke_4.4.0.1009.11
linux-image-powerpc-e500mc_4.4.0.71.77
linux-image-4.4.0-1009-gke_4.4.0-1009.9
linux-image-4.4.0-1051-raspi2_4.4.0-1051.58
linux-image-4.4.0-71-powerpc-smp_4.4.0-71.92
linux-image-4.4.0-71-powerpc-e500mc_4.4.0-71.92
linux-image-lowlatency_4.4.0.71.77
linux-image-generic_4.4.0.71.77
linux-image-4.4.0-71-lowlatency_4.4.0-71.92
linux-image-snapdragon_4.4.0.1054.47
linux-image-4.4.0-71-generic_4.4.0-71.92
linux-image-generic-lpae_4.4.0.71.77
linux-image-aws_4.4.0.1012.15
linux-image-4.4.0-71-powerpc64-smp_4.4.0-71.92
linux-image-4.4.0-1012-aws_4.4.0-1012.21
linux-image-raspi2_4.4.0.1051.52
linux-image-4.4.0-71-generic-lpae_4.4.0-71.92
linux-image-4.4.0-1054-snapdragon_4.4.0-1054.58
linux-image-powerpc64-smp_4.4.0.71.77
linux-image-powerpc-smp_4.4.0.71.77

191885 - Fedora Linux 26 FEDORA-2017-cbed8f4169 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10253

Description

The scan detected that the host is missing the following update:
FEDORA-2017-cbed8f4169

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/2017/4/?count=200&page=3

Fedora Core 26

erlang-19.3-2.fc26

191890 - Fedora Linux 25 FEDORA-2017-42ebcac2b5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10253

Description

The scan detected that the host is missing the following update:
FEDORA-2017-42ebcac2b5

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/2017/3/?count=200&page=1

Fedora Core 25

erlang-19.3-2.fc25

191900 - Fedora Linux 25 FEDORA-2017-93dec9eba5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7184, CVE-2017-7261, CVE-2017-7277

Description

The scan detected that the host is missing the following update:
FEDORA-2017-93dec9eba5

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/2017/4/?count=200&page=1

Fedora Core 25

kernel-4.10.8-200.fc25

191903 - Fedora Linux 26 FEDORA-2017-d5dbc23747 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2641, CVE-2017-2643, CVE-2017-2644, CVE-2017-2645

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d5dbc23747

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/2017/4/?count=200&page=4

Fedora Core 26

moodle-3.2.2-1.fc26

191908 - Fedora Linux 24 FEDORA-2017-0fcaf52f1a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2641, CVE-2017-2643, CVE-2017-2644, CVE-2017-2645

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0fcaf52f1a

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/2017/3/?count=200&page=1

Fedora Core 24

moodle-3.1.5-1.fc24

191910 - Fedora Linux 26 FEDORA-2017-ffc47d48ec Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7567

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ffc47d48ec

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/2017/4/?count=200&page=4

Fedora Core 26

openslp-2.0.0-12.fc26

191911 - Fedora Linux 24 FEDORA-2017-02174df32f Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7184, CVE-2017-7261, CVE-2017-7277

Description

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

FEDORA-2017-02174df32f

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/2017/4/?count=200&page=1

Fedora Core 24

kernel-4.10.8-100.fc24

191913 - Fedora Linux 24 FEDORA-2017-e2480c7f50 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10253

Description

The scan detected that the host is missing the following update:
FEDORA-2017-e2480c7f50

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/2017/3/?count=200&page=1

Fedora Core 24

erlang-18.3.4.5-2.fc24

191914 - Fedora Linux 26 FEDORA-2017-23535a31f8 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6255, CVE-2016-8863

Description

The scan detected that the host is missing the following update:
FEDORA-2017-23535a31f8

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/2017/4/?count=200&page=7

Fedora Core 26

libupnp-1.6.21-1.fc26

191917 - Fedora Linux 25 FEDORA-2017-0196511d58 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2641, CVE-2017-2643, CVE-2017-2644, CVE-2017-2645

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0196511d58

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/2017/4/?count=200&page=7

Fedora Core 25

moodle-3.1.5-1.fc25

21554 - Rockwell Automation FactoryTalk Activation Search Path Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-6015

Description

A vulnerability is present in some versions of Rockwell Automation FactoryTalk Activation.

Observation

Rockwell Automation FactoryTalk Activation is a software application used in energy, manufacturing, and building automation systems.

A vulnerability is present in some versions of Rockwell Automation FactoryTalk Activation. The flaw is due to an uncontrolled search path element. Successful exploitation by an attacker could result in the execution of arbitrary code.

21557 - TrendMicro ServerProtect for Linux 3.0 Cross-Site Scripting Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

A vulnerability is present in some versions of Trend Micro ServerProtect for Linux.

Observation

Trend Micro ServerProtect for Linux provides protection against security risks for file servers based on Linux.

A vulnerability is present in some versions of Trend Micro ServerProtect for Linux. The flaw lies in viewlog.cgi. Successful exploitation could allow an attacker to execute arbitrary code on vulnerable installations.

130738 - Debian Linux 8.0 DSA-3824-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6369

Description

The scan detected that the host is missing the following update:
DSA-3824-1

Observation

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

http://www.debian.org/security/2017/dsa-3824

Debian 8.0
all
firebird2.5-server-common_2.5.3.26778.ds4-5+deb8u1
firebird2.5-superclassic_2.5.3.26778.ds4-5+deb8u1
libib-util_2.5.3.26778.ds4-5+deb8u1
libfbclient2-dbg_2.5.3.26778.ds4-5+deb8u1
firebird2.5-classic-common_2.5.3.26778.ds4-5+deb8u1
firebird2.5-examples_2.5.3.26778.ds4-5+deb8u1
firebird2.5-super-dbg_2.5.3.26778.ds4-5+deb8u1
firebird2.5-common-doc_2.5.3.26778.ds4-5+deb8u1
firebird2.5-classic-dbg_2.5.3.26778.ds4-5+deb8u1
firebird2.5-common_2.5.3.26778.ds4-5+deb8u1
firebird2.5-doc_2.5.3.26778.ds4-5+deb8u1
firebird2.5-classic_2.5.3.26778.ds4-5+deb8u1
firebird2.5-super_2.5.3.26778.ds4-5+deb8u1
firebird-dev_2.5.3.26778.ds4-5+deb8u1
libfbclient2_2.5.3.26778.ds4-5+deb8u1
libfbembed2.5_2.5.3.26778.ds4-5+deb8u1

132345 - Oracle VM OVMSA-2017-0049 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8869

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0049

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000666.html
http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000660.html

OVM3.3
x86_64
ocaml-runtime-3.11.2-5.el6

OVM3.4
x86_64
ocaml-runtime-3.11.2-5.el6

160229 - CentOS 7 CESA-2017-0838 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-5139, CVE-2016-5158, CVE-2016-5159, CVE-2016-7163, CVE-2016-9573, CVE-2016-9675

Description

The scan detected that the host is missing the following update:
CESA-2017-0838

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-March/022349.html

CentOS 7
x86_64
openjpeg-1.5.1-16.el7_3
openjpeg-libs-1.5.1-16.el7_3
openjpeg-devel-1.5.1-16.el7_3

i686
openjpeg-libs-1.5.1-16.el7_3
openjpeg-devel-1.5.1-16.el7_3

170787 - Amazon Linux AMI ALAS-2017-810 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6816, CVE-2016-8745

Description

The scan detected that the host is missing the following update:
ALAS-2017-810

Observation

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

https://alas.aws.amazon.com/ALAS-2017-810.html

Amazon Linux AMI
noarch
tomcat6-webapps-6.0.51-1.10.amzn1
tomcat6-6.0.51-1.10.amzn1
tomcat6-servlet-2.5-api-6.0.51-1.10.amzn1
tomcat6-el-2.1-api-6.0.51-1.10.amzn1
tomcat6-admin-webapps-6.0.51-1.10.amzn1
tomcat6-jsp-2.1-api-6.0.51-1.10.amzn1
tomcat6-docs-webapp-6.0.51-1.10.amzn1
tomcat6-javadoc-6.0.51-1.10.amzn1
tomcat6-lib-6.0.51-1.10.amzn1

191882 - Fedora Linux 24 FEDORA-2017-97d7758431 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6369

Description

The scan detected that the host is missing the following update:
FEDORA-2017-97d7758431

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/2017/4/?count=200&page=1

Fedora Core 24

firebird-2.5.7.27050.0-1.fc24

191884 - Fedora Linux 26 FEDORA-2017-487051ac16 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6060

Description

The scan detected that the host is missing the following update:
FEDORA-2017-487051ac16

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/2017/4/?count=200&page=2

Fedora Core 26

mupdf-1.10a-4.fc26

191887 - Fedora Linux 26 FEDORA-2017-8306577cc7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6429

Description

The scan detected that the host is missing the following update:
FEDORA-2017-8306577cc7

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/2017/4/?count=200&page=2

Fedora Core 26

tcpreplay-4.2.1-1.fc26

191902 - Fedora Linux 24 FEDORA-2017-7980b5e846 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6429

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7980b5e846

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/2017/4/?count=200&page=2

Fedora Core 24

tcpreplay-4.2.1-1.fc24

191906 - Fedora Linux 25 FEDORA-2017-5e945de883 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6429

Description

The scan detected that the host is missing the following update:
FEDORA-2017-5e945de883

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/2017/4/?count=200&page=2

Fedora Core 25

tcpreplay-4.2.1-1.fc25

191909 - Fedora Linux 26 FEDORA-2017-07c8f3ea2b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8714

Description

The scan detected that the host is missing the following update:
FEDORA-2017-07c8f3ea2b

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/2017/4/?count=200&page=5

Fedora Core 26

rkward-0.6.5-5.fc26
R-3.3.3-1.fc26
rpy-2.8.5-3.fc26

191915 - Fedora Linux 26 FEDORA-2017-20d54b2782 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9042, CVE-2017-6451, CVE-2017-6458, CVE-2017-6460, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464

Description

The scan detected that the host is missing the following update:
FEDORA-2017-20d54b2782

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/2017/4/?count=200&page=2

Fedora Core 26

ntp-4.2.8p10-1.fc26

21551 - (K13074505) F5 BIG-IP Libarchive Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-8687

Description

A buffer overflow vulnerability is present in some versions of F5 BIG-IP systems.

Observation

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

A buffer overflow vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the safe_fprintf function in tar/util.c in libarchive. Successful exploitation could allow an attacker to cause a denial of service condition.

21552 - (K52697522) F5 BIG-IP Libarchive Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-8689

Description

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

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A denial of service vulnerability is present in some versions of F5 BIG-IP systems. The flaw lies in the read_Header function in archive_read_support_format_7zip.c in libarchive. Successful exploitation could allow an attacker to cause a denial of service condition.

21553 - LAquis SCADA Path Traversal Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-6020

Description

A vulnerability is present in some versions of LCDS LAquis SCADA.

Observation

LCDS LAquis SCADA is a supervisory control and data acquisition software.

A vulnerability is present in some versions of LCDS LAquis SCADA. The flaw occurs due to improper input validation. Successful exploitation could allow an attacker to obtain sensitive information.

132351 - Oracle VM OVMSA-2017-0052 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2616

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0052

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000667.html
http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000662.html

OVM3.3
x86_64
coreutils-libs-8.4-46.0.1.el6
coreutils-8.4-46.0.1.el6

OVM3.4
x86_64
coreutils-libs-8.4-46.0.1.el6
coreutils-8.4-46.0.1.el6

132354 - Oracle VM OVMSA-2017-0059 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2628

Description

The scan detected that the host is missing the following update:
OVMSA-2017-0059

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000673.html
http://oss.oracle.com/pipermail/oraclevm-errata/2017-March/000672.html

OVM3.3
x86_64
curl-7.19.7-53.el6_9
libcurl-7.19.7-53.el6_9

OVM3.4
x86_64
curl-7.19.7-53.el6_9
libcurl-7.19.7-53.el6_9

141528 - Red Hat Enterprise Linux RHSA-2017-0847 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3148, CVE-2017-2628

Description

The scan detected that the host is missing the following update:
RHSA-2017-0847

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0847.html

RHEL6D
x86_64
curl-7.19.7-53.el6_9
curl-debuginfo-7.19.7-53.el6_9
libcurl-devel-7.19.7-53.el6_9
libcurl-7.19.7-53.el6_9

i386
curl-7.19.7-53.el6_9
curl-debuginfo-7.19.7-53.el6_9
libcurl-devel-7.19.7-53.el6_9
libcurl-7.19.7-53.el6_9

RHEL6S
i386
curl-7.19.7-53.el6_9

curl-debuginfo-7.19.7-53.el6_9
libcurl-devel-7.19.7-53.el6_9
libcurl-7.19.7-53.el6_9

x86_64
curl-7.19.7-53.el6_9
curl-debuginfo-7.19.7-53.el6_9
libcurl-devel-7.19.7-53.el6_9
libcurl-7.19.7-53.el6_9

RHEL6WS
x86_64
curl-7.19.7-53.el6_9
curl-debuginfo-7.19.7-53.el6_9
libcurl-devel-7.19.7-53.el6_9
libcurl-7.19.7-53.el6_9

i386
curl-7.19.7-53.el6_9
curl-debuginfo-7.19.7-53.el6_9
libcurl-devel-7.19.7-53.el6_9
libcurl-7.19.7-53.el6_9

145278 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0853-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10087

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0853-1

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-March/002745.html

SuSE SLED 12 SP1
x86_64
libpng16-debugsource-1.6.8-14.1
libpng16-16-1.6.8-14.1
libpng16-16-debuginfo-1.6.8-14.1
libpng16-16-debuginfo-32bit-1.6.8-14.1
libpng16-16-32bit-1.6.8-14.1

SuSE SLES 12 SP2
x86_64
libpng16-16-32bit-1.6.8-14.1
libpng16-16-1.6.8-14.1
libpng16-16-debuginfo-1.6.8-14.1
libpng16-16-debuginfo-32bit-1.6.8-14.1
libpng16-debugsource-1.6.8-14.1

SuSE SLED 12 SP2
x86_64
libpng16-debugsource-1.6.8-14.1

libpng16-16-1.6.8-14.1
libpng16-16-debuginfo-1.6.8-14.1
libpng16-16-debuginfo-32bit-1.6.8-14.1
libpng16-16-32bit-1.6.8-14.1

SuSE SLES 12 SP1
x86_64
libpng16-16-32bit-1.6.8-14.1
libpng16-16-1.6.8-14.1
libpng16-16-debuginfo-1.6.8-14.1
libpng16-16-debuginfo-32bit-1.6.8-14.1
libpng16-debugsource-1.6.8-14.1

163318 - Oracle Enterprise Linux ELSA-2017-0847 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2628

Description

The scan detected that the host is missing the following update:
ELSA-2017-0847

Observation

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

http://oss.oracle.com/pipermail/el-errata/2017-March/006813.html

OEL6
x86_64
curl-7.19.7-53.el6_9
libcurl-devel-7.19.7-53.el6_9
libcurl-7.19.7-53.el6_9

i386
curl-7.19.7-53.el6_9
libcurl-devel-7.19.7-53.el6_9
libcurl-7.19.7-53.el6_9

191883 - Fedora Linux 26 FEDORA-2017-1be1218e7f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6318

Description

The scan detected that the host is missing the following update:
FEDORA-2017-1be1218e7f

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/2017/4/?count=200&page=2

Fedora Core 26

sane-backends-1.0.25-7.fc26

160230 - CentOS 7 CESA-2017-0837 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5208, CVE-2017-5332, CVE-2017-5333, CVE-2017-6009, CVE-2017-6010, CVE-2017-6011

Description

The scan detected that the host is missing the following update:
CESA-2017-0837

Observation

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

http://lists.centos.org/pipermail/centos-announce/2017-March/022347.html

CentOS 7
x86_64
icoutils-0.31.3-1.el7_3

191899 - Fedora Linux 26 FEDORA-2017-a861eb07ee Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6009, CVE-2017-6010, CVE-2017-6011

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a861eb07ee

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/2017/4/?count=200&page=7

Fedora Core 26

icoutils-0.31.2-1.fc26

191920 - Fedora Linux 26 FEDORA-2017-3456ba4c93 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7261

Description

The scan detected that the host is missing the following update:
FEDORA-2017-3456ba4c93

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/2017/4/?count=200&page=2

Fedora Core 26

kernel-4.11.0-0.rc4.git0.1.fc26

88855 - Slackware Linux 14.0, 14.1, 14.2 SSA:2017-091-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2619

Description

The scan detected that the host is missing the following update:
SSA:2017-091-01

Observation

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

http://www.slackware.com/security/viewer.php?l=slackware-security&y=2017&m=slackware-security.427595

Slackware 14.0
x86_64
samba-4.4.13-x86_64-1

Slackware 14.2
x86_64
samba-4.4.13-x86_64-1

i586
samba-4.4.13-i586-1

Slackware 14.1
x86_64
samba-4.4.13-x86_64-1

130739 - Debian Linux 8.0 DSA-3826-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-0360

Description

The scan detected that the host is missing the following update:
DSA-3826-1

Observation

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

http://www.debian.org/security/2017/dsa-3826

Debian 8.0
all
tryton-server_3.4.0-3+deb8u3

141530 - Red Hat Enterprise Linux RHSA-2017-0861 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2017-0861

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00000.html

RHEL5_6S
i386
redhat-release-5Server-5.6.0.13

x86_64
redhat-release-5Server-5.6.0.13

141531 - Red Hat Enterprise Linux RHSA-2017-0863 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2017-0863

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00002.html

RHEL4ES
x86_64
redhat-release-4ES-10.16

i386
redhat-release-4ES-10.16

RHEL4AS
i386
redhat-release-4AS-10.16

x86_64
redhat-release-4AS-10.16

141532 - Red Hat Enterprise Linux RHSA-2017-0864 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2017-0864

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00003.html

RHEL7_1S
x86_64
redhat-release-server-7.1-1.el7_1.6

141533 - Red Hat Enterprise Linux RHSA-2017-0862 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2017-0862

Observation

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

http://www.redhat.com/archives/enterprise-watch-list/2017-April/msg00001.html

RHEL5D
x86_64
redhat-release-5Client-5.11.0.9

i386
redhat-release-5Client-5.11.0.9

RHEL5S
i386
redhat-release-5Server-5.11.0.9

x86_64
redhat-release-5Server-5.11.0.9

182317 - FreeBSD xen-tools Xenstore Denial Of Service Via Repeated Update (47873d72-14eb-11e7-970f-002590263bf5)

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:
xen-tools -- xenstore denial of service via repeated update (47873d72-14eb-11e7-970f-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/47873d72-14eb-11e7-970f-002590263bf5.html

Affected packages:
xen-tools < 4.7.2_1

182318 - FreeBSD chromium Multiple Vulnerabilities (7cf058d8-158d-11e7-ba2c-e8e0b747a45a)

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

Risk Level: Low

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (7cf058d8-158d-11e7-ba2c-e8e0b747a45a)

Observation

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

http://www.vuxml.org/freebsd/7cf058d8-158d-11e7-ba2c-e8e0b747a45a.html

Affected packages:
chromium < 57.0.2987.133
chromium-npapi < 57.0.2987.133
chromium-pulse < 57.0.2987.133

182319 - FreeBSD django Multible Vulnerabilities (dc880d6c-195d-11e7-8c63-0800277dcc69)

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

Risk Level: Low

CVE: CVE-2017-7233, CVE-2017-7234

Description

The scan detected that the host is missing the following update:
django -- multible vulnerabilities (dc880d6c-195d-11e7-8c63-0800277dcc69)

Observation

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

http://www.vuxml.org/freebsd/dc880d6c-195d-11e7-8c63-0800277dcc69.html

Affected packages:
py27-django < 1.8.18
py33-django < 1.8.18
py34-django < 1.8.18
py35-django < 1.8.18
py36-django < 1.8.18
py27-django18 < 1.8.18
py33-django18 < 1.8.18
py34-django18 < 1.8.18
py35-django18 < 1.8.18
py36-django18 < 1.8.18
py27-django19 < 1.9.13
py33-django19 < 1.9.13
py34-django19 < 1.9.13
py35-django19 < 1.9.13
py36-django19 < 1.9.13
py27-django110 < 1.10.7
py27-django110 < 1.10.7
py27-django110 < 1.10.7
py27-django110 < 1.10.7
py27-django110 < 1.10.7

182320 - FreeBSD asterisk Buffer Overflow In CDR's Set User (356b02e9-1954-11e7-9608-001999f8d30b)

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 -- Buffer overflow in CDR's set user (356b02e9-1954-11e7-9608-001999f8d30b)

Observation

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

http://www.vuxml.org/freebsd/356b02e9-1954-11e7-9608-001999f8d30b.html

Affected packages:
asterisk13 < 13.14.1

182322 - FreeBSD phpMyAdmin Bypass 'no Password' Restriction (68611303-149e-11e7-b9bb-6805ca0b3d42)

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:
phpMyAdmin -- bypass 'no password' restriction (68611303-149e-11e7-b9bb-6805ca0b3d42)

Observation

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

http://www.vuxml.org/freebsd/68611303-149e-11e7-b9bb-6805ca0b3d42.html

Affected packages:
phpMyAdmin < 4.7.0

185646 - Ubuntu Linux 16.04, 16.10 USN-3255-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7358

Description

The scan detected that the host is missing the following update:
USN-3255-1

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-April/003809.html

Ubuntu 16.10

lightdm_1.19.5-0ubuntu1.1

Ubuntu 16.04

lightdm_1.18.3-0ubuntu1.1

185650 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3236-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-5029, CVE-2017-5030, CVE-2017-5031, CVE-2017-5033, CVE-2017-5035, CVE-2017-5037, CVE-2017-5040, CVE-2017-5041, CVE-2017-5044, CVE-2017-5045, CVE-2017-5046

Description

The scan detected that the host is missing the following update:
USN-3236-1

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-March/003797.html

Ubuntu 16.04

liboxideqtcore0_1.21.5-0ubuntu0.16.04.1

Ubuntu 14.04

liboxideqtcore0_1.21.5-0ubuntu0.14.04.1

Ubuntu 16.10

liboxideqtcore0_1.21.5-0ubuntu0.16.10.1

185652 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3242-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
USN-3242-2

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-March/003805.html

Ubuntu 12.04

samba_3.6.25-0ubuntu0.12.04.10

Ubuntu 16.04

samba_4.3.11+dfsg-0ubuntu0.16.04.6

Ubuntu 14.04

samba_4.3.11+dfsg-0ubuntu0.14.04.7

Ubuntu 16.10

samba_4.4.5+dfsg-2ubuntu5.5

185657 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3216-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-5398, CVE-2017-5399, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5403, CVE-2017-5404, CVE-2017-5405, CVE-2017-5406, CVE-2017-5407, CVE-2017-5408, CVE-2017-5410, CVE-2017-5412, CVE-2017-5413, CVE-2017-5414, CVE-2017-5415, CVE-2017-5416, CVE-2017-5417, CVE-2017-5418, CVE-2017-5419, CVE-2017-5420, CVE-2017-5421, CVE-2017-5422, CVE-2017-5426, CVE-2017-5427

Description

The scan detected that the host is missing the following update:
USN-3216-2

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-March/003806.html

Ubuntu 12.04

firefox_52.0.2+build1-0ubuntu0.12.04.1

Ubuntu 16.04

firefox_52.0.2+build1-0ubuntu0.16.04.1

Ubuntu 14.04

firefox_52.0.2+build1-0ubuntu0.14.04.1

Ubuntu 16.10

firefox_52.0.2+build1-0ubuntu0.16.10.1

185658 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3254-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7233, CVE-2017-7234

Description

The scan detected that the host is missing the following update:
USN-3254-1

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-April/003808.html

Ubuntu 12.04

python-django_1.3.1-4ubuntu1.23

Ubuntu 16.04

python-django_1.8.7-1ubuntu5.5
python3-django_1.8.7-1ubuntu5.5

Ubuntu 14.04

python-django_1.6.11-0ubuntu1.1

Ubuntu 16.10

python-django_1.8.7-1ubuntu8.2
python3-django_1.8.7-1ubuntu8.2

191881 - Fedora Linux 26 FEDORA-2017-45ebf1e164 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-2017-45ebf1e164

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/2017/4/?count=200&page=6

Fedora Core 26

knot-resolver-1.2.4-1.fc26

191886 - Fedora Linux 24 FEDORA-2017-7accc8010b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2661

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7accc8010b

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/2017/4/?count=200&page=1

Fedora Core 24

pcs-0.9.156-2.fc24

191888 - Fedora Linux 26 FEDORA-2017-a8add6c46c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-10243

Description

The scan detected that the host is missing the following update:
FEDORA-2017-a8add6c46c

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/2017/4/?count=200&page=1

Fedora Core 26

texlive-2016-33.20160520.fc26

191889 - Fedora Linux 26 FEDORA-2017-718154e0f2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2784

Description

The scan detected that the host is missing the following update:
FEDORA-2017-718154e0f2

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/2017/4/?count=200&page=4

Fedora Core 26

mbedtls-2.4.2-1.fc26

191891 - Fedora Linux 26 FEDORA-2017-3bfbe2acb9 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-2017-3bfbe2acb9

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/2017/4/?count=200&page=6

Fedora Core 26

firefox-52.0-1.fc26

191892 - Fedora Linux 26 FEDORA-2017-b5899f809e 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-b5899f809e

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/2017/4/?count=200&page=3

Fedora Core 26

links-2.14-1.fc26

191893 - Fedora Linux 26 FEDORA-2017-7ac378e011 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2626

Description

The scan detected that the host is missing the following update:
FEDORA-2017-7ac378e011

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/2017/4/?count=200&page=5

Fedora Core 26

libICE-1.0.9-8.fc26

191894 - Fedora Linux 26 FEDORA-2017-8c567ee528 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-2017-8c567ee528

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/2017/4/?count=200&page=1

Fedora Core 26

icecat-52.0.1-5.fc26

191895 - Fedora Linux 26 FEDORA-2017-ffd4a36f09 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-ffd4a36f09

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/2017/4/?count=200&page=6

Fedora Core 26

thunderbird-45.8.0-1.fc26

191896 - Fedora Linux 25 FEDORA-2017-71e69a691b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2661

Description

The scan detected that the host is missing the following update:
FEDORA-2017-71e69a691b

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/2017/4/?count=200&page=1

Fedora Core 25

pcs-0.9.156-2.fc25

191897 - Fedora Linux 25 FEDORA-2017-c22a1dbe8b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2619

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c22a1dbe8b

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/2017/4/?count=200&page=2

Fedora Core 25

samba-4.5.8-0.fc25

191898 - Fedora Linux 26 FEDORA-2017-09f65e5e00 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2625

Description

The scan detected that the host is missing the following update:
FEDORA-2017-09f65e5e00

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/2017/4/?count=200&page=5

Fedora Core 26

libXdmcp-1.1.2-5.fc26

191901 - Fedora Linux 26 FEDORA-2017-b42b86201c 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-b42b86201c

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/2017/4/?count=200&page=2

Fedora Core 26

firefox-52.0-6.fc26

191904 - Fedora Linux 26 FEDORA-2017-b68534e41f 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-b68534e41f

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/2017/4/?count=200&page=3

Fedora Core 26

sscg-2.0.4-1.fc26

191905 - Fedora Linux 26 FEDORA-2017-4a981b2ded 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-2017-4a981b2ded

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/2017/4/?count=200&page=4

Fedora Core 26

drupal8-8.2.7-1.fc26

191907 - Fedora Linux 26 FEDORA-2017-8840ec0204 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-2017-8840ec0204

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/2017/4/?count=200&page=3

Fedora Core 26

empathy-3.12.13-2.fc26

191912 - Fedora Linux 25 FEDORA-2017-ff6940bf63 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ff6940bf63

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/2017/4/?count=200&page=2

Fedora Core 25

chromium-57.0.2987.133-1.fc25

191916 - Fedora Linux 25 FEDORA-2017-d219f0e5fc 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-d219f0e5fc

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/2017/4/?count=200&page=7

Fedora Core 25

sscg-2.0.4-1.fc25

191918 - Fedora Linux 26 FEDORA-2017-da50233929 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-da50233929

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/2017/4/?count=200&page=6

Fedora Core 26

sscg-2.0.3-1.fc26

191919 - Fedora Linux 26 FEDORA-2017-2ae4a42cd4 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-2017-2ae4a42cd4

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/2017/4/?count=200&page=7

Fedora Core 26

wordpress-4.7.3-1.fc26

191921 - Fedora Linux 26 FEDORA-2017-dfaf0ca892 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-dfaf0ca892

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/2017/4/?count=200&page=3

Fedora Core 26

webkitgtk4-2.16.0-1.fc26

191922 - Fedora Linux 24 FEDORA-2017-712ffce24d 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-2017-712ffce24d

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/2017/3/?count=200&page=1

Fedora Core 24

sscg-2.0.4-1.fc24

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.

10765 - WordPress Sniplets Plugin Multiple Cross Site Scripting Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2008-1061

Update Details

FASLScript is updated

191876 - Fedora Linux 24 FEDORA-2017-66593c367e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-6503, CVE-2017-6504

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.