2017-MAR-23
FSL version 7.5.907

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

21303 - (APSB17-05) Vulnerability In Adobe Digital Editions

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

Risk Level: High

CVE: CVE-2017-2973, CVE-2017-2974, CVE-2017-2975, CVE-2017-2976, CVE-2017-2977, CVE-2017-2978, CVE-2017-2979, CVE-2017-2980, CVE-2017-2981

Description

Multiple vulnerabilities are present in some versions of Adobe Digital Editions.

Observation

Adobe Digital Editions is the Adobe's eBook reader software.

Multiple vulnerabilities are present in some versions of Adobe Digital Editions. The flaws are due to some buffer overflow conditions. Successful exploitation by an attacker could cause a memory leak, or lead to arbitrary code execution.

21304 - (APSB17-05) Vulnerability In Adobe Digital Editions

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-2973, CVE-2017-2974, CVE-2017-2975, CVE-2017-2976, CVE-2017-2977, CVE-2017-2978, CVE-2017-2979, CVE-2017-2980, CVE-2017-2981

Description

Multiple vulnerabilities are present in some versions of Adobe Digital Editions.

Observation

Adobe Digital Editions is the Adobe's eBook reader software.

Multiple vulnerabilities are present in some versions of Adobe Digital Editions. The flaws are due to some buffer overflow conditions. Successful exploitation by an attacker could cause a memory leak, or lead to arbitrary code execution.

141518 - Red Hat Enterprise Linux RHSA-2017-0526 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2997, CVE-2017-2998, CVE-2017-2999, CVE-2017-3000, CVE-2017-3001, CVE-2017-3002, CVE-2017-3003

Description

The scan detected that the host is missing the following update:
RHSA-2017-0526

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0526.html

RHEL6D
x86_64
flash-plugin-25.0.0.127-1.el6_8

i386
flash-plugin-25.0.0.127-1.el6_8

RHEL6S
x86_64
flash-plugin-25.0.0.127-1.el6_8

i386
flash-plugin-25.0.0.127-1.el6_8

RHEL6WS
x86_64
flash-plugin-25.0.0.127-1.el6_8

i386
flash-plugin-25.0.0.127-1.el6_8

145262 - SuSE SLED 12 SP1 SUSE-SU-2017:0703-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2997, CVE-2017-2998, CVE-2017-2999, CVE-2017-3000, CVE-2017-3001, CVE-2017-3002, CVE-2017-3003

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0703-1

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/002698.html

SuSE SLED 12 SP1
x86_64
flash-player-gnome-25.0.0.127-162.1
flash-player-25.0.0.127-162.1

178415 - Gentoo Linux GLSA-201703-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-2997, CVE-2017-2998, CVE-2017-2999, CVE-2017-3000, CVE-2017-3001, CVE-2017-3002, CVE-2017-3003

Description

The scan detected that the host is missing the following update:
GLSA-201703-02

Observation

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

https://security.gentoo.org/glsa/201703-02

Affected packages:
www-plugins/adobe-flash < 25.0.0.127

182312 - FreeBSD Flash Player Multiple Vulnerabilities (4ffb633c-0a3b-11e7-a9f2-0011d823eebd)

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

Risk Level: High

CVE: CVE-2017-2997, CVE-2017-2998, CVE-2017-2999, CVE-2017-3000, CVE-2017-3001, CVE-2017-3002, CVE-2017-3003

Description

The scan detected that the host is missing the following update:
Flash Player -- multiple vulnerabilities (4ffb633c-0a3b-11e7-a9f2-0011d823eebd)

Observation

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

http://www.vuxml.org/freebsd/4ffb633c-0a3b-11e7-a9f2-0011d823eebd.html

Affected packages:
linux-flashplayer < 25.0.0.127

185627 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3235-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4448, CVE-2016-4658, CVE-2016-5131

Description

The scan detected that the host is missing the following update:
USN-3235-1

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/003780.html

Ubuntu 12.04

libxml2_2.7.8.dfsg-5.1ubuntu4.17

Ubuntu 16.04

libxml2_2.9.3+dfsg1-1ubuntu0.2

Ubuntu 14.04

libxml2_2.9.1+dfsg1-3ubuntu4.9

Ubuntu 16.10

libxml2_2.9.4+dfsg1-2ubuntu0.1

21321 - NetIQ Access Manager Prior To 4.3 SP1

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

Risk Level: High

CVE: CVE-2017-5183

Description

A vulnerability is present in some versions of NetIQ Access Manager.

Observation

NetIQ Access Manager is a simple and secure solution for access needs.

A vulnerability is present in some versions of NetIQ Access Manager. The flaw lies in the SAML Assertion Consumer Service (ACS) whitelist functionality. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

21322 - NetIQ Access Manager Prior To 4.3 SP1

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-5183

Description

A vulnerability is present in some versions of NetIQ Access Manager.

Observation

NetIQ Access Manager is a simple and secure solution for access needs.

A vulnerability is present in some versions of NetIQ Access Manager. The flaw lies in the SAML Assertion Consumer Service (ACS) whitelist functionality. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

141512 - Red Hat Enterprise Linux RHSA-2017-0558 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5428

Description

The scan detected that the host is missing the following update:
RHSA-2017-0558

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0558.html

RHEL7D
x86_64
firefox-debuginfo-52.0-5.el7_3
firefox-52.0-5.el7_3

RHEL7S
x86_64
firefox-debuginfo-52.0-5.el7_3
firefox-52.0-5.el7_3

RHEL7WS
x86_64
firefox-debuginfo-52.0-5.el7_3
firefox-52.0-5.el7_3

160228 - CentOS 7 CESA-2017-0558 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5428

Description

The scan detected that the host is missing the following update:
CESA-2017-0558

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/022344.html

CentOS 7
x86_64
firefox-52.0-5.el7.centos

i686
firefox-52.0-5.el7.centos

163299 - Oracle Enterprise Linux ELSA-2017-0558 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5428

Description

The scan detected that the host is missing the following update:
ELSA-2017-0558

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/006787.html

OEL7
x86_64
firefox-52.0-5.0.1.el7_3

175130 - Scientific Linux Security ERRATA Critical: firefox on SL7.x x86_64 (1703-8844)

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

Risk Level: High

CVE: CVE-2017-5428

Description

The scan detected that the host is missing the following update:
Security ERRATA Critical: firefox on SL7.x x86_64 (1703-8844)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1703&L=scientific-linux-errata&F=&S=&P=8844

SL7
x86_64
firefox-debuginfo-52.0-5.el7_3
firefox-52.0-5.el7_3

21315 - IBM WebSphere Message Broker Denial Of Service Vulnerability (swg21997918)

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

Risk Level: High

CVE: CVE-2016-9706

Description

A denial-of-service vulnerability is present in some versions of IBM WebSphere Message Broker.

Observation

IBM WebSphere Message Broker is a popular advanced Enterprise Service Bus.

A denial-of-service vulnerability is present in some versions of IBM WebSphere Message Broker. The flaw lies in how this product handles XML data. Successful exploitation could allow a remote attacker to cause a denial-of-service or expose highly sensitive information.

21302 - (K68401558) F5 BIG-IP Virtual Server TCP Sequence Numbers Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2002-1463

Description

A vulnerability is present in some versions of F5's BIG-IP Products.

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's BIG-IP Products. The flaw is present in the BIG-IP virtual servers. Successful exploitation could allow a malicious user to conduct spoofing attacks.

21317 - IBM WebSphere MQ Multiple OpenSSL Vulnerabilities (swg21998797)

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

Risk Level: High

CVE: CVE-2016-2106, CVE-2016-2109

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere MQ.

Observation

IBM WebSphere MQ is a messaging solution.

Multiple vulnerabilities are present in some versions of IBM WebSphere MQ. The flaw lies in the OpenSSL component. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial-of-service.

21327 - (K73926196) F5 BIG-IP PHPMailer Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-10045

Description

A remote code execution vulnerability is present in some versions of F5's BIG-IP Products.

Observation

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

A remote code execution vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in the PHPMailer component. Successful exploitation could allow an attacker to remotely execute arbitrary code, disclose sensitive information or cause a denial of service.

21387 - IBM WebSphere MQ Administration Command Denial Of Service Vulnerability

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

Risk Level: High

CVE: CVE-2016-8971

Description

A denial of service vulnerability is present in some versions of IBM WebSphere MQ.

Observation

IBM WebSphere MQ is a popular cross platform messaging system.

A denial of service vulnerability is present in some versions of IBM WebSphere MQ. The flaw is due to an invalid memory access caused by an administration command. Successful exploitation by a remote attacker could result in a denial of service condition.

21492 - (VMSA-2017-0003) VMware Workstation Pro Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-4898, CVE-2017-4899, CVE-2017-4900

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Pro.

Observation

VMware Workstation is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Pro. The flaws lie in multiple components. Successful exploitation could allow an attacker to cause a denial of service, escalate privileges to System in the host machine.

21506 - Wireshark Multiple Vulnerabilities Prior To 2.0.11

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

Risk Level: High

CVE: CVE-2017-6014, CVE-2017-6467, CVE-2017-6468, CVE-2017-6469, CVE-2017-6470, CVE-2017-6471, CVE-2017-6472, CVE-2017-6473, CVE-2017-6474

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a tool that is used to analyze the network protocol and traffic.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause a denial of service condition.

21507 - Wireshark Multiple Vulnerabilities Prior To 2.2.5

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

Risk Level: High

CVE: CVE-2017-6014, CVE-2017-6467, CVE-2017-6468, CVE-2017-6469, CVE-2017-6470, CVE-2017-6471, CVE-2017-6472, CVE-2017-6473, CVE-2017-6474

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

Wireshark is a tool that is used to analyze the network protocol and traffic.

Multiple vulnerabilities are present in some versions of Wireshark. The flaws lie in multiple dissectors. Successful exploitation could allow an attacker to cause a denial of service condition.

21510 - Mozilla Thunderbird 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-2017-5410

Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

Mozilla Thunderbird is an open-source email, newsgroup, news feed, and chat client.

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird. 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.

21511 - Mozilla Thunderbird 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-2017-5410

Description

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird.

Observation

Mozilla Thunderbird is an open-source email, newsgroup, news feed, and chat client.

Multiple vulnerabilities are present in some versions of Mozilla Thunderbird. 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.

21513 - IBM WebSphere MQ Denial-Of-Service Vulnerability (swg21999672)

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

Risk Level: High

CVE: CVE-2017-1145

Description

A denial of service vulnerability is present in some versions of IBM WebSphere MQ.

Observation

IBM WebSphere MQ is a popular cross platform messaging system.

A denial of service vulnerability is present in some versions of IBM WebSphere MQ. The flaw occurs due to improper termination of channel agents by IBM WebSphere MQ. Successful exploitation could allow an attacker to cause a denial of service condition.

21517 - WordPress Multiple Vulnerabilities Prior To 4.7.3

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of WordPress.

Observation

WordPress is a popular blog application.

Multiple vulnerabilities are present in some versions of WordPress. The flaws lie in multiple components. Successful exploitation could allow an attacker to remotely execute arbitrary code.

21531 - IBM WebSphere MQ Multiple OpenSSL Vulnerabilities (swg21999724)

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

Risk Level: High

CVE: CVE-2016-2177, CVE-2016-2178

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere MQ.

Observation

IBM WebSphere MQ is a popular cross platform messaging system.

Multiple vulnerabilities are present in some versions of IBM WebSphere MQ. The flaws lie in OpenSSL component. Successful exploitation could allow an attacker to retrieve sensitive data, cause a denial of service condition or have other unspecified impact on the target system.

130725 - Debian Linux 8.0 DSA-3811-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5596, CVE-2017-5597, CVE-2017-6014, CVE-2017-6467, CVE-2017-6468, CVE-2017-6469, CVE-2017-6470, CVE-2017-6471, CVE-2017-6472, CVE-2017-6473, CVE-2017-6474

Description

The scan detected that the host is missing the following update:
DSA-3811-1

Observation

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

http://www.debian.org/security/2017/dsa-3811

Debian 8.0
all
wireshark_1.12.1+g01b65bf-4+deb8u11

141505 - Red Hat Enterprise Linux RHSA-2017-0559 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-6045, CVE-2016-5139, CVE-2016-5158, CVE-2016-5159, CVE-2016-7163, CVE-2016-9675

Description

The scan detected that the host is missing the following update:
RHSA-2017-0559

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0559.html

RHEL6D
x86_64
openjpeg-debuginfo-1.3-16.el6_8
openjpeg-devel-1.3-16.el6_8
openjpeg-libs-1.3-16.el6_8
openjpeg-1.3-16.el6_8

i386
openjpeg-debuginfo-1.3-16.el6_8
openjpeg-devel-1.3-16.el6_8
openjpeg-libs-1.3-16.el6_8
openjpeg-1.3-16.el6_8

RHEL6S
i386
openjpeg-debuginfo-1.3-16.el6_8
openjpeg-devel-1.3-16.el6_8
openjpeg-libs-1.3-16.el6_8
openjpeg-1.3-16.el6_8

x86_64
openjpeg-debuginfo-1.3-16.el6_8
openjpeg-devel-1.3-16.el6_8
openjpeg-libs-1.3-16.el6_8
openjpeg-1.3-16.el6_8

RHEL6WS
x86_64
openjpeg-debuginfo-1.3-16.el6_8
openjpeg-libs-1.3-16.el6_8

i386
openjpeg-debuginfo-1.3-16.el6_8
openjpeg-libs-1.3-16.el6_8

141508 - Red Hat Enterprise Linux RHSA-2017-0535 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7545

Description

The scan detected that the host is missing the following update:
RHSA-2017-0535

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0535.html

RHEL7_2S
x86_64
policycoreutils-2.2.5-21.el7_2
policycoreutils-newrole-2.2.5-21.el7_2
policycoreutils-gui-2.2.5-21.el7_2
policycoreutils-sandbox-2.2.5-21.el7_2
policycoreutils-restorecond-2.2.5-21.el7_2
policycoreutils-debuginfo-2.2.5-21.el7_2
policycoreutils-devel-2.2.5-21.el7_2
policycoreutils-python-2.2.5-21.el7_2

141509 - Red Hat Enterprise Linux RHSA-2017-0680 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2017-0680

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0680.html

RHEL6D
x86_64
glibc-debuginfo-2.12-1.209.el6
glibc-common-2.12-1.209.el6
glibc-2.12-1.209.el6
glibc-static-2.12-1.209.el6
glibc-headers-2.12-1.209.el6
nscd-2.12-1.209.el6
glibc-utils-2.12-1.209.el6
glibc-devel-2.12-1.209.el6
glibc-debuginfo-common-2.12-1.209.el6

i386
glibc-debuginfo-2.12-1.209.el6
glibc-common-2.12-1.209.el6
glibc-2.12-1.209.el6
glibc-static-2.12-1.209.el6
glibc-headers-2.12-1.209.el6
nscd-2.12-1.209.el6
glibc-utils-2.12-1.209.el6
glibc-devel-2.12-1.209.el6
glibc-debuginfo-common-2.12-1.209.el6

RHEL6S
i386
glibc-debuginfo-2.12-1.209.el6
glibc-common-2.12-1.209.el6
glibc-2.12-1.209.el6
glibc-static-2.12-1.209.el6

glibc-headers-2.12-1.209.el6
nscd-2.12-1.209.el6
glibc-utils-2.12-1.209.el6
glibc-devel-2.12-1.209.el6
glibc-debuginfo-common-2.12-1.209.el6

x86_64
glibc-debuginfo-2.12-1.209.el6
glibc-common-2.12-1.209.el6
glibc-2.12-1.209.el6
glibc-static-2.12-1.209.el6
glibc-headers-2.12-1.209.el6
nscd-2.12-1.209.el6
glibc-utils-2.12-1.209.el6
glibc-devel-2.12-1.209.el6
glibc-debuginfo-common-2.12-1.209.el6

RHEL6WS
x86_64
glibc-debuginfo-2.12-1.209.el6
glibc-common-2.12-1.209.el6
glibc-2.12-1.209.el6
glibc-headers-2.12-1.209.el6
nscd-2.12-1.209.el6
glibc-utils-2.12-1.209.el6
glibc-devel-2.12-1.209.el6
glibc-debuginfo-common-2.12-1.209.el6

i386
glibc-debuginfo-2.12-1.209.el6
glibc-common-2.12-1.209.el6
glibc-2.12-1.209.el6
glibc-headers-2.12-1.209.el6
nscd-2.12-1.209.el6
glibc-utils-2.12-1.209.el6
glibc-devel-2.12-1.209.el6
glibc-debuginfo-common-2.12-1.209.el6

141516 - Red Hat Enterprise Linux RHSA-2017-0794 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2013-2236, CVE-2016-1245, CVE-2016-2342, CVE-2016-4049, CVE-2017-5495

Description

The scan detected that the host is missing the following update:
RHSA-2017-0794

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0794.html

RHEL6S
i386
quagga-debuginfo-0.99.15-14.el6
quagga-contrib-0.99.15-14.el6

quagga-devel-0.99.15-14.el6
quagga-0.99.15-14.el6

x86_64
quagga-debuginfo-0.99.15-14.el6
quagga-contrib-0.99.15-14.el6
quagga-devel-0.99.15-14.el6
quagga-0.99.15-14.el6

RHEL6WS
x86_64
quagga-0.99.15-14.el6
quagga-debuginfo-0.99.15-14.el6

i386
quagga-0.99.15-14.el6
quagga-debuginfo-0.99.15-14.el6

RHEL6D
x86_64
quagga-debuginfo-0.99.15-14.el6
quagga-contrib-0.99.15-14.el6
quagga-devel-0.99.15-14.el6

i386
quagga-debuginfo-0.99.15-14.el6
quagga-contrib-0.99.15-14.el6
quagga-devel-0.99.15-14.el6

141517 - Red Hat Enterprise Linux RHSA-2017-0536 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7545

Description

The scan detected that the host is missing the following update:
RHSA-2017-0536

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0536.html

RHEL7_1S
x86_64
policycoreutils-devel-2.2.5-16.el7_1
policycoreutils-debuginfo-2.2.5-16.el7_1
policycoreutils-python-2.2.5-16.el7_1
policycoreutils-restorecond-2.2.5-16.el7_1
policycoreutils-gui-2.2.5-16.el7_1
policycoreutils-sandbox-2.2.5-16.el7_1
policycoreutils-2.2.5-16.el7_1
policycoreutils-newrole-2.2.5-16.el7_1

141519 - Red Hat Enterprise Linux RHSA-2017-0631 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise 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:
RHSA-2017-0631

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0631.html

RHEL6D
x86_64
wireshark-debuginfo-1.8.10-25.el6
wireshark-gnome-1.8.10-25.el6
wireshark-devel-1.8.10-25.el6
wireshark-1.8.10-25.el6

i386
wireshark-debuginfo-1.8.10-25.el6
wireshark-gnome-1.8.10-25.el6
wireshark-devel-1.8.10-25.el6
wireshark-1.8.10-25.el6

RHEL6S
i386
wireshark-debuginfo-1.8.10-25.el6
wireshark-gnome-1.8.10-25.el6
wireshark-devel-1.8.10-25.el6
wireshark-1.8.10-25.el6

x86_64
wireshark-debuginfo-1.8.10-25.el6
wireshark-gnome-1.8.10-25.el6
wireshark-devel-1.8.10-25.el6
wireshark-1.8.10-25.el6

RHEL6WS
x86_64
wireshark-debuginfo-1.8.10-25.el6
wireshark-gnome-1.8.10-25.el6
wireshark-1.8.10-25.el6

i386
wireshark-debuginfo-1.8.10-25.el6
wireshark-gnome-1.8.10-25.el6
wireshark-1.8.10-25.el6

141521 - Red Hat Enterprise Linux RHSA-2017-0641 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8325

Description

The scan detected that the host is missing the following update:
RHSA-2017-0641

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0641.html

RHEL6D
x86_64
openssh-5.3p1-122.el6
openssh-debuginfo-5.3p1-122.el6
pam_ssh_agent_auth-0.9.3-122.el6
openssh-server-5.3p1-122.el6
openssh-ldap-5.3p1-122.el6
openssh-clients-5.3p1-122.el6
openssh-askpass-5.3p1-122.el6

i386
openssh-5.3p1-122.el6
openssh-debuginfo-5.3p1-122.el6
pam_ssh_agent_auth-0.9.3-122.el6
openssh-server-5.3p1-122.el6
openssh-ldap-5.3p1-122.el6
openssh-clients-5.3p1-122.el6
openssh-askpass-5.3p1-122.el6

RHEL6S
i386
openssh-5.3p1-122.el6
openssh-debuginfo-5.3p1-122.el6
pam_ssh_agent_auth-0.9.3-122.el6
openssh-server-5.3p1-122.el6
openssh-ldap-5.3p1-122.el6
openssh-clients-5.3p1-122.el6
openssh-askpass-5.3p1-122.el6

x86_64
openssh-5.3p1-122.el6
openssh-debuginfo-5.3p1-122.el6
pam_ssh_agent_auth-0.9.3-122.el6
openssh-server-5.3p1-122.el6
openssh-ldap-5.3p1-122.el6
openssh-clients-5.3p1-122.el6
openssh-askpass-5.3p1-122.el6

RHEL6WS
x86_64
openssh-clients-5.3p1-122.el6
openssh-server-5.3p1-122.el6
openssh-askpass-5.3p1-122.el6
openssh-5.3p1-122.el6
openssh-debuginfo-5.3p1-122.el6

i386
openssh-clients-5.3p1-122.el6
openssh-server-5.3p1-122.el6

openssh-askpass-5.3p1-122.el6
openssh-5.3p1-122.el6
openssh-debuginfo-5.3p1-122.el6

141524 - Red Hat Enterprise Linux RHSA-2017-0725 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
RHSA-2017-0725

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0725.html

RHEL6D
x86_64
bash-doc-4.1.2-48.el6
bash-debuginfo-4.1.2-48.el6
bash-4.1.2-48.el6

i386
bash-doc-4.1.2-48.el6
bash-debuginfo-4.1.2-48.el6
bash-4.1.2-48.el6

RHEL6S
i386
bash-doc-4.1.2-48.el6
bash-debuginfo-4.1.2-48.el6
bash-4.1.2-48.el6

x86_64
bash-doc-4.1.2-48.el6
bash-debuginfo-4.1.2-48.el6
bash-4.1.2-48.el6

RHEL6WS
x86_64
bash-4.1.2-48.el6
bash-debuginfo-4.1.2-48.el6

i386
bash-4.1.2-48.el6
bash-debuginfo-4.1.2-48.el6

141525 - Red Hat Enterprise Linux RHSA-2017-0817 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10088, CVE-2016-10142, CVE-2016-2069, CVE-2016-2384, CVE-2016-6480, CVE-2016-7042, CVE-2016-7097, CVE-2016-8399, CVE-2016-9576

Description

The scan detected that the host is missing the following update:
RHSA-2017-0817

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0817.html

RHEL6D
i386
perf-debuginfo-2.6.32-696.el6
kernel-2.6.32-696.el6
python-perf-2.6.32-696.el6
perf-2.6.32-696.el6
kernel-debug-2.6.32-696.el6
kernel-debuginfo-2.6.32-696.el6
kernel-debuginfo-common-i686-2.6.32-696.el6
python-perf-debuginfo-2.6.32-696.el6
kernel-headers-2.6.32-696.el6
kernel-debug-debuginfo-2.6.32-696.el6
kernel-debug-devel-2.6.32-696.el6
kernel-devel-2.6.32-696.el6

noarch
kernel-firmware-2.6.32-696.el6
kernel-abi-whitelists-2.6.32-696.el6
kernel-doc-2.6.32-696.el6

x86_64
python-perf-2.6.32-696.el6
kernel-debug-2.6.32-696.el6
python-perf-debuginfo-2.6.32-696.el6
perf-2.6.32-696.el6
kernel-debuginfo-common-x86_64-2.6.32-696.el6
kernel-2.6.32-696.el6
kernel-headers-2.6.32-696.el6
kernel-debug-debuginfo-2.6.32-696.el6
kernel-debuginfo-common-i686-2.6.32-696.el6
perf-debuginfo-2.6.32-696.el6
kernel-devel-2.6.32-696.el6
kernel-debug-devel-2.6.32-696.el6
kernel-debuginfo-2.6.32-696.el6

RHEL6S
i386
perf-debuginfo-2.6.32-696.el6
kernel-2.6.32-696.el6
python-perf-2.6.32-696.el6
perf-2.6.32-696.el6
kernel-debug-2.6.32-696.el6
kernel-debuginfo-2.6.32-696.el6
kernel-debuginfo-common-i686-2.6.32-696.el6
python-perf-debuginfo-2.6.32-696.el6
kernel-headers-2.6.32-696.el6
kernel-debug-debuginfo-2.6.32-696.el6
kernel-debug-devel-2.6.32-696.el6
kernel-devel-2.6.32-696.el6

noarch
kernel-firmware-2.6.32-696.el6
kernel-abi-whitelists-2.6.32-696.el6
kernel-doc-2.6.32-696.el6

x86_64
python-perf-2.6.32-696.el6
kernel-debug-2.6.32-696.el6
python-perf-debuginfo-2.6.32-696.el6
perf-2.6.32-696.el6
kernel-debuginfo-common-x86_64-2.6.32-696.el6
kernel-2.6.32-696.el6
kernel-headers-2.6.32-696.el6
kernel-debug-debuginfo-2.6.32-696.el6
kernel-debuginfo-common-i686-2.6.32-696.el6
perf-debuginfo-2.6.32-696.el6
kernel-devel-2.6.32-696.el6
kernel-debug-devel-2.6.32-696.el6
kernel-debuginfo-2.6.32-696.el6

RHEL6WS
i386
perf-debuginfo-2.6.32-696.el6
kernel-2.6.32-696.el6
perf-2.6.32-696.el6
kernel-debug-2.6.32-696.el6
kernel-debuginfo-2.6.32-696.el6
kernel-debuginfo-common-i686-2.6.32-696.el6
python-perf-debuginfo-2.6.32-696.el6
kernel-headers-2.6.32-696.el6
kernel-debug-debuginfo-2.6.32-696.el6
kernel-debug-devel-2.6.32-696.el6
kernel-devel-2.6.32-696.el6

noarch
kernel-firmware-2.6.32-696.el6
kernel-abi-whitelists-2.6.32-696.el6
kernel-doc-2.6.32-696.el6

x86_64
perf-debuginfo-2.6.32-696.el6
kernel-2.6.32-696.el6
perf-2.6.32-696.el6
kernel-debuginfo-common-x86_64-2.6.32-696.el6
kernel-debug-2.6.32-696.el6
kernel-debuginfo-2.6.32-696.el6
kernel-debuginfo-common-i686-2.6.32-696.el6
python-perf-debuginfo-2.6.32-696.el6
kernel-headers-2.6.32-696.el6
kernel-debug-debuginfo-2.6.32-696.el6
kernel-debug-devel-2.6.32-696.el6
kernel-devel-2.6.32-696.el6

145257 - SuSE SLES 11 SP4 SUSE-SU-2017:0717-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6318

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0717-1

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/002704.html

SuSE SLES 11 SP4
i586
sane-backends-1.0.20-7.8.1

x86_64
sane-backends-1.0.20-7.8.1

145258 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2017:0701-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5191

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0701-1

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/002696.html

SuSE SLES 12 SP1
x86_64
libvmtools0-10.1.0-5.3.1
open-vm-tools-desktop-10.1.0-5.3.1
libvmtools0-debuginfo-10.1.0-5.3.1
open-vm-tools-debuginfo-10.1.0-5.3.1
open-vm-tools-debugsource-10.1.0-5.3.1
open-vm-tools-10.1.0-5.3.1
open-vm-tools-desktop-debuginfo-10.1.0-5.3.1

SuSE SLED 12 SP1
x86_64
libvmtools0-10.1.0-5.3.1
open-vm-tools-desktop-10.1.0-5.3.1
libvmtools0-debuginfo-10.1.0-5.3.1
open-vm-tools-debuginfo-10.1.0-5.3.1
open-vm-tools-debugsource-10.1.0-5.3.1
open-vm-tools-10.1.0-5.3.1
open-vm-tools-desktop-debuginfo-10.1.0-5.3.1

145259 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0714-1 Update Is Not Installed

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

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

The scan detected that the host is missing the following update:
SUSE-SU-2017:0714-1

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/002701.html

SuSE SLED 12 SP1
x86_64
MozillaFirefox-45.8.0esr-102.1
MozillaFirefox-translations-45.8.0esr-102.1
MozillaFirefox-debugsource-45.8.0esr-102.1
MozillaFirefox-debuginfo-45.8.0esr-102.1

SuSE SLES 12 SP2
x86_64
MozillaFirefox-45.8.0esr-102.1
MozillaFirefox-translations-45.8.0esr-102.1
MozillaFirefox-debugsource-45.8.0esr-102.1
MozillaFirefox-debuginfo-45.8.0esr-102.1

SuSE SLED 12 SP2
x86_64
MozillaFirefox-45.8.0esr-102.1
MozillaFirefox-translations-45.8.0esr-102.1
MozillaFirefox-debugsource-45.8.0esr-102.1
MozillaFirefox-debuginfo-45.8.0esr-102.1

SuSE SLES 12 SP1
x86_64
MozillaFirefox-45.8.0esr-102.1
MozillaFirefox-translations-45.8.0esr-102.1
MozillaFirefox-debugsource-45.8.0esr-102.1
MozillaFirefox-debuginfo-45.8.0esr-102.1

145260 - SuSE SLES 11 SP4 SUSE-SU-2017:0732-1 Update Is Not Installed

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

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

The scan detected that the host is missing the following update:
SUSE-SU-2017:0732-1

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/002712.html

SuSE SLES 11 SP4
i586
MozillaFirefox-45.8.0esr-68.1
MozillaFirefox-translations-45.8.0esr-68.1

x86_64
MozillaFirefox-45.8.0esr-68.1
MozillaFirefox-translations-45.8.0esr-68.1

145261 - SuSE SLES 11 SP4 SUSE-SU-2017:0705-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5191

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0705-1

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/002699.html

SuSE SLES 11 SP4
x86_64
libvmtools0-10.1.0-7.1
open-vm-tools-10.1.0-7.1
open-vm-tools-desktop-10.1.0-7.1

i586
libvmtools0-10.1.0-7.1
open-vm-tools-10.1.0-7.1
open-vm-tools-desktop-10.1.0-7.1

145263 - SuSE SLED 12 SP2 SUSE-SU-2017:0694-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-4433

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0694-1

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/002693.html

SuSE SLED 12 SP2
x86_64

libgegl-0_2-0-debuginfo-0.2.0-14.3
gegl-0_2-0.2.0-14.3
gegl-0_2-debuginfo-0.2.0-14.3
gegl-debugsource-0.2.0-14.3
gegl-debuginfo-0.2.0-14.3
libgegl-0_2-0-0.2.0-14.3

noarch
gegl-0_2-lang-0.2.0-14.3

145266 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0713-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6318

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0713-1

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/002700.html

SuSE SLED 12 SP2
x86_64
sane-backends-32bit-1.0.24-3.1
sane-backends-1.0.24-3.1
sane-backends-debuginfo-32bit-1.0.24-3.1
sane-backends-autoconfig-1.0.24-3.1
sane-backends-debugsource-1.0.24-3.1
sane-backends-debuginfo-1.0.24-3.1

SuSE SLES 12 SP2
x86_64
sane-backends-debuginfo-1.0.24-3.1
sane-backends-debugsource-1.0.24-3.1
sane-backends-1.0.24-3.1

SuSE SLES 12 SP1
x86_64
sane-backends-debuginfo-1.0.24-3.1
sane-backends-debugsource-1.0.24-3.1
sane-backends-1.0.24-3.1

SuSE SLED 12 SP1
x86_64
sane-backends-32bit-1.0.24-3.1
sane-backends-1.0.24-3.1
sane-backends-debuginfo-32bit-1.0.24-3.1
sane-backends-autoconfig-1.0.24-3.1
sane-backends-debugsource-1.0.24-3.1
sane-backends-debuginfo-1.0.24-3.1

145268 - SuSE SLED 12 SP1 SUSE-SU-2017:0696-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2012-4433

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0696-1

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/002695.html

SuSE SLED 12 SP1
x86_64
gegl-debugsource-0.2.0-10.3.3
gegl-0_2-debuginfo-0.2.0-10.3.3
libgegl-0_2-0-debuginfo-0.2.0-10.3.3
gegl-debuginfo-0.2.0-10.3.3
gegl-0_2-0.2.0-10.3.3
libgegl-0_2-0-0.2.0-10.3.3

noarch
gegl-0_2-lang-0.2.0-10.3.3

145269 - SuSE SLES 11 SP4 SUSE-SU-2017:0729-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2161, CVE-2016-8743

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0729-1

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/002710.html

SuSE SLES 11 SP4
i586
apache2-2.2.12-69.1
apache2-example-pages-2.2.12-69.1
apache2-doc-2.2.12-69.1
apache2-utils-2.2.12-69.1
apache2-prefork-2.2.12-69.1
apache2-worker-2.2.12-69.1

x86_64
apache2-2.2.12-69.1
apache2-example-pages-2.2.12-69.1
apache2-doc-2.2.12-69.1
apache2-utils-2.2.12-69.1

apache2-prefork-2.2.12-69.1
apache2-worker-2.2.12-69.1

145270 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:0702-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5191

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0702-1

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/002697.html

SuSE SLED 12 SP2
x86_64
open-vm-tools-debuginfo-10.1.0-8.1
open-vm-tools-desktop-10.1.0-8.1
libvmtools0-debuginfo-10.1.0-8.1
open-vm-tools-10.1.0-8.1
open-vm-tools-debugsource-10.1.0-8.1
libvmtools0-10.1.0-8.1
open-vm-tools-desktop-debuginfo-10.1.0-8.1

SuSE SLES 12 SP2
x86_64
open-vm-tools-debuginfo-10.1.0-8.1
open-vm-tools-desktop-10.1.0-8.1
libvmtools0-debuginfo-10.1.0-8.1
open-vm-tools-10.1.0-8.1
open-vm-tools-debugsource-10.1.0-8.1
libvmtools0-10.1.0-8.1
open-vm-tools-desktop-debuginfo-10.1.0-8.1

160227 - CentOS 5, 6, 7 CESA-2017-0498 Update Is Not Installed

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

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-2017-5410

Description

The scan detected that the host is missing the following update:
CESA-2017-0498

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/022338.html
http://lists.centos.org/pipermail/centos-announce/2017-March/022339.html

http://lists.centos.org/pipermail/centos-announce/2017-March/022340.html

CentOS 6
x86_64
thunderbird-45.8.0-1.el6.centos

i686
thunderbird-45.8.0-1.el6.centos

CentOS 7
x86_64
thunderbird-45.8.0-1.el7.centos

CentOS 5
x86_64
thunderbird-45.8.0-1.el5.centos

i386
thunderbird-45.8.0-1.el5.centos

175131 - Scientific Linux Security ERRATA Moderate: openjpeg on SL6.x i386/x86_64 (1703-9169)

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

Risk Level: High

CVE: CVE-2013-6045, CVE-2016-5139, CVE-2016-5158, CVE-2016-5159, CVE-2016-7163, CVE-2016-9675

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: openjpeg on SL6.x i386/x86_64 (1703-9169)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1703&L=scientific-linux-errata&F=&S=&P=9169

SL6
x86_64
openjpeg-debuginfo-1.3-16.el6_8
openjpeg-devel-1.3-16.el6_8
openjpeg-libs-1.3-16.el6_8
openjpeg-1.3-16.el6_8

i386
openjpeg-debuginfo-1.3-16.el6_8
openjpeg-devel-1.3-16.el6_8
openjpeg-libs-1.3-16.el6_8
openjpeg-1.3-16.el6_8

182309 - FreeBSD moodle Multiple Vulnerabilities (f72d98d1-0b7e-11e7-970f-002590263bf5)

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

Risk Level: High

CVE: CVE-2016-10045, CVE-2017-2576, CVE-2017-2578

Description

The scan detected that the host is missing the following update:
moodle -- multiple vulnerabilities (f72d98d1-0b7e-11e7-970f-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/f72d98d1-0b7e-11e7-970f-002590263bf5.html

Affected packages:
moodle29 <= 2.9.9
moodle30 < 3.0.8
moodle31 < 3.1.4
moodle32 < 3.2.1

185632 - Ubuntu Linux 12.04, 14.04, 16.04 USN-3239-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5180, CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2016-3706, CVE-2016-4429, CVE-2016-5417, CVE-2016-6323

Description

The scan detected that the host is missing the following update:
USN-3239-2

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/003787.html

Ubuntu 12.04

libc6_2.15-0ubuntu10.17

Ubuntu 16.04

libc6_2.23-0ubuntu7

Ubuntu 14.04

libc6_2.19-0ubuntu6.11

185635 - Ubuntu Linux 12.04, 14.04, 16.04 USN-3239-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5180, CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2016-3706, CVE-2016-4429, CVE-2016-5417, CVE-2016-6323

Description

The scan detected that the host is missing the following update:
USN-3239-1

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/003786.html

Ubuntu 12.04

libc6_2.15-0ubuntu10.16

Ubuntu 16.04

libc6_2.23-0ubuntu6

Ubuntu 14.04

libc6_2.19-0ubuntu6.10

191847 - Fedora Linux 25 FEDORA-2017-534e23bad9 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9877

Description

The scan detected that the host is missing the following update:
FEDORA-2017-534e23bad9

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=2

Fedora Core 25

rabbitmq-server-3.6.6-2.fc25

21331 - (K08383757) F5 BIG-IP perl-XML-Twig Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-9180

Description

A vulnerability is present in some versions of F5's BIG-IP Products.

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's BIG-IP Products. The flaw lies in the perl XML Twig library. Successful exploitation could allow a local attacker to disclose information or cause a denial of service condition.

21498 - DotCMS Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-3187, CVE-2017-3188, CVE-2017-3189

Description

Multiple vulnerabilities are present in some versions of dotCMS Enterprise Pro.

Observation

dotCMS is a content management system (CMS) for managing content and content driven sites and applications.

Multiple vulnerabilities are present in some versions of dotCMS Enterprise Pro. The flaws lie in the administrator panel and the Push Publishing feature. Successful exploitation could allow an attacker to write files to arbitrary directories on the file system, perform actions with the dotCMS administrator panel, and execute arbitrary system commands.

21516 - (VMSA-2017-0003) VMware Workstation Player Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-4898, CVE-2017-4899, CVE-2017-4900

Description

Multiple vulnerabilities are present in some versions of VMware Workstation Player.

Observation

VMware Workstation Player is a virtualization software.

Multiple vulnerabilities are present in some versions of VMware Workstation Player. The flaws lie in several components. Successful exploitation could allow a local attacker to escalate privileges or cause a denial of service condition.

21542 - (SB10185) McAfee Data Loss Prevention Endpoint Access Control Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-8012

Description

A vulnerability is present in some versions of McAfee Data Loss Prevention Endpoint.

Observation

McAfee Data Loss Prevention Endpoint is a security tool to safeguard intellectual property and protect intellectual data via system policies.

A vulnerability is present in some versions of McAfee Data Loss Prevention Endpoint. The flaw lies in how objects are handled in memory. Successful exploitation could allow an attacker to affect confidentiality, integrity and availability.

130726 - Debian Linux 8.0 DSA-3813-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8714

Description

The scan detected that the host is missing the following update:
DSA-3813-1

Observation

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

http://www.debian.org/security/2017/dsa-3813

Debian 8.0
all
r-base_3.1.1-1+deb8u1

141507 - Red Hat Enterprise Linux RHSA-2017-0630 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10207, CVE-2017-5581

Description

The scan detected that the host is missing the following update:
RHSA-2017-0630

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0630.html

RHEL6D
i386
tigervnc-server-1.1.0-24.el6
tigervnc-1.1.0-24.el6
tigervnc-debuginfo-1.1.0-24.el6
tigervnc-server-module-1.1.0-24.el6

noarch
tigervnc-server-applet-1.1.0-24.el6

x86_64
tigervnc-server-1.1.0-24.el6
tigervnc-1.1.0-24.el6
tigervnc-debuginfo-1.1.0-24.el6
tigervnc-server-module-1.1.0-24.el6

RHEL6S
i386
tigervnc-server-1.1.0-24.el6
tigervnc-1.1.0-24.el6
tigervnc-debuginfo-1.1.0-24.el6
tigervnc-server-module-1.1.0-24.el6

noarch
tigervnc-server-applet-1.1.0-24.el6

x86_64

tigervnc-server-1.1.0-24.el6
tigervnc-1.1.0-24.el6
tigervnc-debuginfo-1.1.0-24.el6
tigervnc-server-module-1.1.0-24.el6

RHEL6WS
x86_64
tigervnc-server-1.1.0-24.el6
tigervnc-1.1.0-24.el6
tigervnc-debuginfo-1.1.0-24.el6

i386
tigervnc-server-1.1.0-24.el6
tigervnc-1.1.0-24.el6
tigervnc-debuginfo-1.1.0-24.el6

141510 - Red Hat Enterprise Linux RHSA-2017-0565 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8869

Description

The scan detected that the host is missing the following update:
RHSA-2017-0565

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0565.html

RHEL6D
x86_64
ocaml-labltk-3.11.2-5.el6
ocaml-emacs-3.11.2-5.el6
ocaml-ocamldoc-3.11.2-5.el6
ocaml-debuginfo-3.11.2-5.el6
ocaml-x11-3.11.2-5.el6
ocaml-source-3.11.2-5.el6
ocaml-runtime-3.11.2-5.el6
ocaml-3.11.2-5.el6
ocaml-camlp4-3.11.2-5.el6
ocaml-camlp4-devel-3.11.2-5.el6
ocaml-labltk-devel-3.11.2-5.el6
ocaml-docs-3.11.2-5.el6

i386
ocaml-labltk-3.11.2-5.el6
ocaml-emacs-3.11.2-5.el6
ocaml-ocamldoc-3.11.2-5.el6
ocaml-debuginfo-3.11.2-5.el6
ocaml-x11-3.11.2-5.el6
ocaml-source-3.11.2-5.el6
ocaml-runtime-3.11.2-5.el6
ocaml-3.11.2-5.el6
ocaml-camlp4-3.11.2-5.el6
ocaml-camlp4-devel-3.11.2-5.el6

ocaml-labltk-devel-3.11.2-5.el6
ocaml-docs-3.11.2-5.el6

RHEL6S
i386
ocaml-labltk-3.11.2-5.el6
ocaml-emacs-3.11.2-5.el6
ocaml-ocamldoc-3.11.2-5.el6
ocaml-debuginfo-3.11.2-5.el6
ocaml-x11-3.11.2-5.el6
ocaml-source-3.11.2-5.el6
ocaml-runtime-3.11.2-5.el6
ocaml-3.11.2-5.el6
ocaml-camlp4-3.11.2-5.el6
ocaml-camlp4-devel-3.11.2-5.el6
ocaml-labltk-devel-3.11.2-5.el6
ocaml-docs-3.11.2-5.el6

x86_64
ocaml-labltk-3.11.2-5.el6
ocaml-emacs-3.11.2-5.el6
ocaml-ocamldoc-3.11.2-5.el6
ocaml-debuginfo-3.11.2-5.el6
ocaml-x11-3.11.2-5.el6
ocaml-source-3.11.2-5.el6
ocaml-runtime-3.11.2-5.el6
ocaml-3.11.2-5.el6
ocaml-camlp4-3.11.2-5.el6
ocaml-camlp4-devel-3.11.2-5.el6
ocaml-labltk-devel-3.11.2-5.el6
ocaml-docs-3.11.2-5.el6

141523 - Red Hat Enterprise Linux RHSA-2017-0564 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8869

Description

The scan detected that the host is missing the following update:
RHSA-2017-0564

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0564.html

RHEL6D
x86_64
ocaml-libguestfs-devel-1.20.11-20.el6
libguestfs-java-1.20.11-20.el6
perl-Sys-Guestfs-1.20.11-20.el6
libguestfs-tools-1.20.11-20.el6
libguestfs-devel-1.20.11-20.el6
libguestfs-java-devel-1.20.11-20.el6
python-libguestfs-1.20.11-20.el6
ocaml-libguestfs-1.20.11-20.el6

ruby-libguestfs-1.20.11-20.el6
libguestfs-debuginfo-1.20.11-20.el6
libguestfs-tools-c-1.20.11-20.el6
libguestfs-javadoc-1.20.11-20.el6
libguestfs-1.20.11-20.el6

RHEL6S
x86_64
ocaml-libguestfs-devel-1.20.11-20.el6
libguestfs-java-1.20.11-20.el6
perl-Sys-Guestfs-1.20.11-20.el6
libguestfs-tools-1.20.11-20.el6
libguestfs-devel-1.20.11-20.el6
libguestfs-java-devel-1.20.11-20.el6
python-libguestfs-1.20.11-20.el6
ocaml-libguestfs-1.20.11-20.el6
ruby-libguestfs-1.20.11-20.el6
libguestfs-debuginfo-1.20.11-20.el6
libguestfs-tools-c-1.20.11-20.el6
libguestfs-javadoc-1.20.11-20.el6
libguestfs-1.20.11-20.el6

RHEL6WS
x86_64
libguestfs-tools-1.20.11-20.el6
python-libguestfs-1.20.11-20.el6
perl-Sys-Guestfs-1.20.11-20.el6
libguestfs-debuginfo-1.20.11-20.el6
libguestfs-tools-c-1.20.11-20.el6
libguestfs-1.20.11-20.el6
libguestfs-java-1.20.11-20.el6

160225 - CentOS 6 CESA-2017-0559 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-2016-9675

Description

The scan detected that the host is missing the following update:
CESA-2017-0559

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/022343.html

CentOS 6
x86_64
openjpeg-libs-1.3-16.el6_8
openjpeg-devel-1.3-16.el6_8
openjpeg-1.3-16.el6_8

i686
openjpeg-libs-1.3-16.el6_8
openjpeg-devel-1.3-16.el6_8
openjpeg-1.3-16.el6_8

163301 - Oracle Enterprise Linux ELSA-2017-0559 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
ELSA-2017-0559

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/006788.html

OEL6
x86_64
openjpeg-libs-1.3-16.el6_8
openjpeg-devel-1.3-16.el6_8
openjpeg-1.3-16.el6_8

i386
openjpeg-libs-1.3-16.el6_8
openjpeg-devel-1.3-16.el6_8
openjpeg-1.3-16.el6_8

178414 - Gentoo Linux GLSA-201703-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1513

Description

The scan detected that the host is missing the following update:
GLSA-201703-01

Observation

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

https://security.gentoo.org/glsa/201703-01

Affected packages:
app-office/openoffice-bin < 4.1.3

185630 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3237-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10244

Description

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

USN-3237-1

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/003782.html

Ubuntu 12.04

libfreetype6_2.4.8-1ubuntu2.4

Ubuntu 16.04

libfreetype6_2.6.1-0.1ubuntu2.1

Ubuntu 14.04

libfreetype6_2.5.2-1ubuntu2.6

Ubuntu 16.10

libfreetype6_2.6.3-3ubuntu1.1

191838 - Fedora Linux 24 FEDORA-2017-783e8fa63e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9422, CVE-2016-9423, CVE-2016-9424, CVE-2016-9425, CVE-2016-9426, CVE-2016-9428, CVE-2016-9429, CVE-2016-9430, CVE-2016-9431, CVE-2016-9432, CVE-2016-9433, CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633

Description

The scan detected that the host is missing the following update:
FEDORA-2017-783e8fa63e

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

w3m-0.5.3-30.git20170102.fc24

191839 - Fedora Linux 25 FEDORA-2017-dc1828d4f9 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-dc1828d4f9

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=2

Fedora Core 25

tcpreplay-4.1.2-3.fc25

191845 - Fedora Linux 25 FEDORA-2017-ae18216e75 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-ae18216e75

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

rkward-0.6.5-5.fc25
R-3.3.3-1.fc25
rpy-2.8.5-3.fc25

191851 - Fedora Linux 24 FEDORA-2017-da9d0f0dc0 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-da9d0f0dc0

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

rkward-0.6.5-5.fc24
rpy-2.8.5-3.fc24
R-3.3.3-1.fc24

191855 - Fedora Linux 24 FEDORA-2017-936a79ee30 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-2017-936a79ee30

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=2

Fedora Core 24

tcpreplay-4.1.2-3.fc24

21297 - (SB10183) McAfee Agent Denial Of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-3896

Description

A vulnerability is present in some versions of McAfee Agent.

Observation

McAfee Agent is client software used to communicate with McAfee ePolicy Orchestrator.

A vulnerability is present in some versions of McAfee Agent. The flaw lies in the validation of input within the remote log viewing functionality. Successful exploitation could allow an attacker to cause a denial of service condition.

21325 - (K22216037) F5 BIG-IP TMM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-9245

Description

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

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 products. The flaw is due to improper handling of malicious requests made to virtual servers. Successful exploitation could allow an attacker to cause a denial of service condition.

21328 - Novell iManager Vulnerability Prior To 2.7 Support Pack 7 Patch 9

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

Risk Level: Medium

CVE: CVE-2017-5186

Description

A vulnerability is present in some versions of Novell (NetIQ) iManager.

Observation

Novell iManager is a web-based administration console.

A vulnerability is present in some versions of Novell (NetIQ) iManager. The flaw lies in the connection with Sentinel server. Successful exploitation results in failing to connect with Sentinel 7.4.2 and above version.

21332 - Novell iManager Vulnerability Prior To 3.0.2.1

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

Risk Level: Medium

CVE: CVE-2017-5186

Description

A vulnerability is present in some versions of Novell (NetIQ) iManager.

Observation

Novell iManager is a web-based administration console.

A vulnerability is present in some versions of Novell (NetIQ) iManager. The flaw lies in the connection with Sentinel. Successful exploitation results in failing to connect Sentinel 7.4.2 and above version.

21493 - LibreOffice Calc and Writer Arbitrary File Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-3157

Description

An Arbitrary file disclosure vulnerability is present in some versions of LibreOffice.

Observation

LibreOffice is an open source office suite.

An Arbitrary file disclosure vulnerability is present in some versions of LibreOffice.The flaw lies in the handling of a crafted document with embedded object. Successful exploitation by an attacker could result in the disclosure of sensitive information.

21495 - LibreOffice Calc and Writer Arbitrary File Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2017-3157

Description

An Arbitrary file disclosure vulnerability is present in some versions of LibreOffice.

Observation

LibreOffice is an open source office suite.

An Arbitrary file disclosure vulnerability is present in some versions of LibreOffice.The flaw lies in the handling of a crafted document with embedded object. Successful exploitation by an attacker could result in the disclosure of sensitive information.

21499 - (K04450715) F5 BIG-IP Libxml2 Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-8806

Description

A denial of service 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 denial of service vulnerability is present in some versions of F5's BIG-IP products. The flaw lies in dict.c in libxml2. Successful exploitation could allow an attacker to cause a denial of service condition.

21528 - Cisco Nexus 5000, 6000, and 7000 Series Switches Software IS-IS Packet Processing Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-3804

Description

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

Observation

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

A vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to improper processing of a crafted IS-IS packet. Successful exploitation could allow an attacker to cause a denial of service condition.

21533 - Apache Tomcat Vulnerability Prior To 9.0.0.M17

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

Risk Level: Medium

CVE: CVE-2016-8747

Description

An information disclosure vulnerability is present in some versions of Apache Tomcat.

Observation

Apache Tomcat is a container for the Java Servlet and Java Server Pages Web applications.

An information disclosure vulnerability is present in some versions of Apache Tomcat. The flaw lies in all HTTP connectors and applies when reverse-proxy configurations are enabled. Successful exploitation could allow an attacker to access potentially sensitive information.

21536 - Cisco Nexus 9000 Series Switches Telnet Login Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-3878

Description

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

Observation

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

A denial of service vulnerability is present in some versions of Cisco NX-OS Software. The flaw is due to incomplete input validation of Telnet packet headers. Successful exploitation could allow an attacker to cause a denial of service condition.

130723 - Debian Linux 8.0 DSA-3809-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3302, CVE-2017-3313

Description

The scan detected that the host is missing the following update:
DSA-3809-1

Observation

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

http://www.debian.org/security/2017/dsa-3809

Debian 8.0
all
mariadb-server_10.0.30-0+deb8u1
mariadb-common_10.0.30-0+deb8u1
libmariadbd-dev_10.0.30-0+deb8u1
mariadb-server-core-10.0_10.0.30-0+deb8u1
mariadb-client-core-10.0_10.0.30-0+deb8u1
mariadb-connect-engine-10.0_10.0.30-0+deb8u1
mariadb-client-10.0_10.0.30-0+deb8u1
mariadb-test-10.0_10.0.30-0+deb8u1
mariadb-server-10.0_10.0.30-0+deb8u1
mariadb-test_10.0.30-0+deb8u1
mariadb-oqgraph-engine-10.0_10.0.30-0+deb8u1
mariadb-client_10.0.30-0+deb8u1

141506 - Red Hat Enterprise Linux RHSA-2017-0698 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4455

Description

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

RHSA-2017-0698

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0698.html

RHEL6D
i386
python-rhsm-certificates-1.18.6-1.el6
subscription-manager-firstboot-1.18.10-1.el6
python-rhsm-1.18.6-1.el6
subscription-manager-migration-1.18.10-1.el6
subscription-manager-1.18.10-1.el6
subscription-manager-plugin-container-1.18.10-1.el6
subscription-manager-debuginfo-1.18.10-1.el6
subscription-manager-gui-1.18.10-1.el6
python-rhsm-debuginfo-1.18.6-1.el6

noarch
subscription-manager-migration-data-2.0.34-1.el6

x86_64
python-rhsm-certificates-1.18.6-1.el6
subscription-manager-firstboot-1.18.10-1.el6
python-rhsm-1.18.6-1.el6
subscription-manager-migration-1.18.10-1.el6
subscription-manager-1.18.10-1.el6
subscription-manager-plugin-container-1.18.10-1.el6
subscription-manager-debuginfo-1.18.10-1.el6
subscription-manager-gui-1.18.10-1.el6
python-rhsm-debuginfo-1.18.6-1.el6

RHEL6S
i386
python-rhsm-certificates-1.18.6-1.el6
subscription-manager-firstboot-1.18.10-1.el6
python-rhsm-1.18.6-1.el6
subscription-manager-migration-1.18.10-1.el6
subscription-manager-1.18.10-1.el6
subscription-manager-plugin-container-1.18.10-1.el6
subscription-manager-debuginfo-1.18.10-1.el6
subscription-manager-gui-1.18.10-1.el6
python-rhsm-debuginfo-1.18.6-1.el6

noarch
subscription-manager-migration-data-2.0.34-1.el6

x86_64
python-rhsm-certificates-1.18.6-1.el6
subscription-manager-firstboot-1.18.10-1.el6
python-rhsm-1.18.6-1.el6
subscription-manager-migration-1.18.10-1.el6
subscription-manager-1.18.10-1.el6
subscription-manager-plugin-container-1.18.10-1.el6
subscription-manager-debuginfo-1.18.10-1.el6
subscription-manager-gui-1.18.10-1.el6
python-rhsm-debuginfo-1.18.6-1.el6

RHEL6WS
i386
python-rhsm-certificates-1.18.6-1.el6
subscription-manager-firstboot-1.18.10-1.el6
python-rhsm-1.18.6-1.el6
subscription-manager-migration-1.18.10-1.el6
subscription-manager-1.18.10-1.el6
subscription-manager-debuginfo-1.18.10-1.el6
subscription-manager-gui-1.18.10-1.el6
python-rhsm-debuginfo-1.18.6-1.el6

noarch
subscription-manager-migration-data-2.0.34-1.el6

x86_64
python-rhsm-certificates-1.18.6-1.el6
subscription-manager-firstboot-1.18.10-1.el6
python-rhsm-1.18.6-1.el6
subscription-manager-migration-1.18.10-1.el6
subscription-manager-1.18.10-1.el6
subscription-manager-debuginfo-1.18.10-1.el6
subscription-manager-gui-1.18.10-1.el6
python-rhsm-debuginfo-1.18.6-1.el6

141511 - Red Hat Enterprise Linux RHSA-2017-0527 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise 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:
RHSA-2017-0527

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0527.html

RHEL6S
noarch
tomcat6-servlet-2.5-api-6.0.24-105.el6_8
tomcat6-jsp-2.1-api-6.0.24-105.el6_8
tomcat6-6.0.24-105.el6_8
tomcat6-lib-6.0.24-105.el6_8
tomcat6-el-2.1-api-6.0.24-105.el6_8
tomcat6-webapps-6.0.24-105.el6_8
tomcat6-admin-webapps-6.0.24-105.el6_8
tomcat6-javadoc-6.0.24-105.el6_8
tomcat6-docs-webapp-6.0.24-105.el6_8

RHEL6WS
noarch
tomcat6-el-2.1-api-6.0.24-105.el6_8
tomcat6-lib-6.0.24-105.el6_8
tomcat6-jsp-2.1-api-6.0.24-105.el6_8
tomcat6-servlet-2.5-api-6.0.24-105.el6_8

tomcat6-6.0.24-105.el6_8

RHEL6D
noarch
tomcat6-servlet-2.5-api-6.0.24-105.el6_8
tomcat6-javadoc-6.0.24-105.el6_8
tomcat6-6.0.24-105.el6_8
tomcat6-lib-6.0.24-105.el6_8
tomcat6-el-2.1-api-6.0.24-105.el6_8
tomcat6-webapps-6.0.24-105.el6_8
tomcat6-admin-webapps-6.0.24-105.el6_8
tomcat6-docs-webapp-6.0.24-105.el6_8
tomcat6-jsp-2.1-api-6.0.24-105.el6_8

141513 - Red Hat Enterprise Linux RHSA-2017-0654 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2616

Description

The scan detected that the host is missing the following update:
RHSA-2017-0654

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0654.html

RHEL6D
x86_64
coreutils-libs-8.4-46.el6
coreutils-8.4-46.el6
coreutils-debuginfo-8.4-46.el6

i386
coreutils-libs-8.4-46.el6
coreutils-8.4-46.el6
coreutils-debuginfo-8.4-46.el6

RHEL6S
i386
coreutils-libs-8.4-46.el6
coreutils-8.4-46.el6
coreutils-debuginfo-8.4-46.el6

x86_64
coreutils-libs-8.4-46.el6
coreutils-8.4-46.el6
coreutils-debuginfo-8.4-46.el6

RHEL6WS
x86_64
coreutils-libs-8.4-46.el6
coreutils-8.4-46.el6
coreutils-debuginfo-8.4-46.el6

i386
coreutils-libs-8.4-46.el6
coreutils-8.4-46.el6
coreutils-debuginfo-8.4-46.el6

141514 - Red Hat Enterprise Linux RHSA-2017-0662 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2125, CVE-2016-2126

Description

The scan detected that the host is missing the following update:
RHSA-2017-0662

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0662.html

RHEL6D
x86_64
samba-winbind-clients-3.6.23-41.el6
samba-glusterfs-3.6.23-41.el6
libsmbclient-3.6.23-41.el6
samba-swat-3.6.23-41.el6
samba-winbind-3.6.23-41.el6
samba-winbind-krb5-locator-3.6.23-41.el6
libsmbclient-devel-3.6.23-41.el6
samba-common-3.6.23-41.el6
samba-doc-3.6.23-41.el6
samba-debuginfo-3.6.23-41.el6
samba-winbind-devel-3.6.23-41.el6
samba-client-3.6.23-41.el6
samba-domainjoin-gui-3.6.23-41.el6
samba-3.6.23-41.el6

i386
samba-winbind-clients-3.6.23-41.el6
libsmbclient-3.6.23-41.el6
samba-swat-3.6.23-41.el6
samba-winbind-3.6.23-41.el6
samba-winbind-krb5-locator-3.6.23-41.el6
libsmbclient-devel-3.6.23-41.el6
samba-common-3.6.23-41.el6
samba-doc-3.6.23-41.el6
samba-debuginfo-3.6.23-41.el6
samba-winbind-devel-3.6.23-41.el6
samba-client-3.6.23-41.el6
samba-domainjoin-gui-3.6.23-41.el6
samba-3.6.23-41.el6

RHEL6S
i386
samba-winbind-clients-3.6.23-41.el6
libsmbclient-3.6.23-41.el6
samba-swat-3.6.23-41.el6

samba-winbind-3.6.23-41.el6
samba-winbind-krb5-locator-3.6.23-41.el6
libsmbclient-devel-3.6.23-41.el6
samba-common-3.6.23-41.el6
samba-doc-3.6.23-41.el6
samba-debuginfo-3.6.23-41.el6
samba-winbind-devel-3.6.23-41.el6
samba-client-3.6.23-41.el6
samba-domainjoin-gui-3.6.23-41.el6
samba-3.6.23-41.el6

x86_64
samba-winbind-clients-3.6.23-41.el6
samba-glusterfs-3.6.23-41.el6
libsmbclient-3.6.23-41.el6
samba-swat-3.6.23-41.el6
samba-winbind-3.6.23-41.el6
samba-winbind-krb5-locator-3.6.23-41.el6
libsmbclient-devel-3.6.23-41.el6
samba-common-3.6.23-41.el6
samba-doc-3.6.23-41.el6
samba-debuginfo-3.6.23-41.el6
samba-winbind-devel-3.6.23-41.el6
samba-client-3.6.23-41.el6
samba-domainjoin-gui-3.6.23-41.el6
samba-3.6.23-41.el6

RHEL6WS
x86_64
samba-3.6.23-41.el6
samba-common-3.6.23-41.el6
samba-debuginfo-3.6.23-41.el6
samba-winbind-clients-3.6.23-41.el6
libsmbclient-3.6.23-41.el6
samba-client-3.6.23-41.el6
samba-winbind-3.6.23-41.el6

i386
samba-3.6.23-41.el6
samba-common-3.6.23-41.el6
samba-debuginfo-3.6.23-41.el6
samba-winbind-clients-3.6.23-41.el6
libsmbclient-3.6.23-41.el6
samba-client-3.6.23-41.el6
samba-winbind-3.6.23-41.el6

141515 - Red Hat Enterprise Linux RHSA-2017-0744 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2125, CVE-2016-2126

Description

The scan detected that the host is missing the following update:
RHSA-2017-0744

Observation

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

For more information see:

https://rhn.redhat.com/errata/RHSA-2017-0744.html

RHEL6D
x86_64
samba4-dc-libs-4.2.10-9.el6
samba4-test-4.2.10-9.el6
samba4-devel-4.2.10-9.el6
samba4-winbind-krb5-locator-4.2.10-9.el6
samba4-common-4.2.10-9.el6
samba4-winbind-4.2.10-9.el6
samba4-client-4.2.10-9.el6
samba4-winbind-clients-4.2.10-9.el6
samba4-dc-4.2.10-9.el6
samba4-pidl-4.2.10-9.el6
samba4-libs-4.2.10-9.el6
samba4-debuginfo-4.2.10-9.el6
samba4-python-4.2.10-9.el6
samba4-4.2.10-9.el6

i386
samba4-dc-libs-4.2.10-9.el6
samba4-test-4.2.10-9.el6
samba4-devel-4.2.10-9.el6
samba4-winbind-krb5-locator-4.2.10-9.el6
samba4-common-4.2.10-9.el6
samba4-winbind-4.2.10-9.el6
samba4-client-4.2.10-9.el6
samba4-winbind-clients-4.2.10-9.el6
samba4-dc-4.2.10-9.el6
samba4-pidl-4.2.10-9.el6
samba4-libs-4.2.10-9.el6
samba4-debuginfo-4.2.10-9.el6
samba4-python-4.2.10-9.el6
samba4-4.2.10-9.el6

RHEL6S
i386
samba4-dc-libs-4.2.10-9.el6
samba4-test-4.2.10-9.el6
samba4-devel-4.2.10-9.el6
samba4-winbind-krb5-locator-4.2.10-9.el6
samba4-common-4.2.10-9.el6
samba4-winbind-4.2.10-9.el6
samba4-client-4.2.10-9.el6
samba4-winbind-clients-4.2.10-9.el6
samba4-dc-4.2.10-9.el6
samba4-pidl-4.2.10-9.el6
samba4-libs-4.2.10-9.el6
samba4-debuginfo-4.2.10-9.el6
samba4-python-4.2.10-9.el6
samba4-4.2.10-9.el6

x86_64
samba4-dc-libs-4.2.10-9.el6
samba4-test-4.2.10-9.el6
samba4-devel-4.2.10-9.el6
samba4-winbind-krb5-locator-4.2.10-9.el6
samba4-common-4.2.10-9.el6

samba4-winbind-4.2.10-9.el6
samba4-client-4.2.10-9.el6
samba4-winbind-clients-4.2.10-9.el6
samba4-dc-4.2.10-9.el6
samba4-pidl-4.2.10-9.el6
samba4-libs-4.2.10-9.el6
samba4-debuginfo-4.2.10-9.el6
samba4-python-4.2.10-9.el6
samba4-4.2.10-9.el6

RHEL6WS
x86_64
samba4-dc-libs-4.2.10-9.el6
samba4-test-4.2.10-9.el6
samba4-devel-4.2.10-9.el6
samba4-winbind-krb5-locator-4.2.10-9.el6
samba4-common-4.2.10-9.el6
samba4-winbind-4.2.10-9.el6
samba4-client-4.2.10-9.el6
samba4-winbind-clients-4.2.10-9.el6
samba4-dc-4.2.10-9.el6
samba4-pidl-4.2.10-9.el6
samba4-libs-4.2.10-9.el6
samba4-debuginfo-4.2.10-9.el6
samba4-python-4.2.10-9.el6
samba4-4.2.10-9.el6

i386
samba4-dc-libs-4.2.10-9.el6
samba4-test-4.2.10-9.el6
samba4-devel-4.2.10-9.el6
samba4-winbind-krb5-locator-4.2.10-9.el6
samba4-common-4.2.10-9.el6
samba4-winbind-4.2.10-9.el6
samba4-client-4.2.10-9.el6
samba4-winbind-clients-4.2.10-9.el6
samba4-dc-4.2.10-9.el6
samba4-pidl-4.2.10-9.el6
samba4-libs-4.2.10-9.el6
samba4-debuginfo-4.2.10-9.el6
samba4-python-4.2.10-9.el6
samba4-4.2.10-9.el6

141522 - Red Hat Enterprise Linux RHSA-2017-0574 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8610, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337

Description

The scan detected that the host is missing the following update:
RHSA-2017-0574

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0574.html

RHEL6D
x86_64
gnutls-debuginfo-2.12.23-21.el6
gnutls-2.12.23-21.el6
gnutls-guile-2.12.23-21.el6
gnutls-devel-2.12.23-21.el6
gnutls-utils-2.12.23-21.el6

i386
gnutls-debuginfo-2.12.23-21.el6
gnutls-2.12.23-21.el6
gnutls-guile-2.12.23-21.el6
gnutls-devel-2.12.23-21.el6
gnutls-utils-2.12.23-21.el6

RHEL6S
i386
gnutls-debuginfo-2.12.23-21.el6
gnutls-2.12.23-21.el6
gnutls-guile-2.12.23-21.el6
gnutls-devel-2.12.23-21.el6
gnutls-utils-2.12.23-21.el6

x86_64
gnutls-debuginfo-2.12.23-21.el6
gnutls-2.12.23-21.el6
gnutls-guile-2.12.23-21.el6
gnutls-devel-2.12.23-21.el6
gnutls-utils-2.12.23-21.el6

RHEL6WS
x86_64
gnutls-debuginfo-2.12.23-21.el6
gnutls-2.12.23-21.el6
gnutls-devel-2.12.23-21.el6
gnutls-utils-2.12.23-21.el6

i386
gnutls-debuginfo-2.12.23-21.el6
gnutls-2.12.23-21.el6
gnutls-devel-2.12.23-21.el6
gnutls-utils-2.12.23-21.el6

145256 - SuSE SLES 11 SP4 SUSE-SU-2017:0719-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2183

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0719-1

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/002706.html

SuSE SLES 11 SP4
i586
java-1_7_1-ibm-plugin-1.7.1_sr4.1-22.1
java-1_7_1-ibm-alsa-1.7.1_sr4.1-22.1
java-1_7_1-ibm-1.7.1_sr4.1-22.1
java-1_7_1-ibm-jdbc-1.7.1_sr4.1-22.1

x86_64
java-1_7_1-ibm-plugin-1.7.1_sr4.1-22.1
java-1_7_1-ibm-alsa-1.7.1_sr4.1-22.1
java-1_7_1-ibm-1.7.1_sr4.1-22.1
java-1_7_1-ibm-jdbc-1.7.1_sr4.1-22.1

145264 - SuSE SLES 11 SP4 SUSE-SU-2017:0731-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3200, CVE-2016-1000212

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0731-1

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/002711.html

SuSE SLES 11 SP4
i586
lighttpd-1.4.20-2.58.1

x86_64
lighttpd-1.4.20-2.58.1

145267 - SuSE SLES 12 SP1, 12 SP2 SUSE-SU-2017:0720-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2183

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0720-1

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/002707.html

SuSE SLES 12 SP1
x86_64
java-1_7_1-ibm-jdbc-1.7.1_sr4.1-34.1

java-1_7_1-ibm-plugin-1.7.1_sr4.1-34.1
java-1_7_1-ibm-1.7.1_sr4.1-34.1
java-1_7_1-ibm-alsa-1.7.1_sr4.1-34.1

SuSE SLES 12 SP2
x86_64
java-1_7_1-ibm-jdbc-1.7.1_sr4.1-34.1
java-1_7_1-ibm-plugin-1.7.1_sr4.1-34.1
java-1_7_1-ibm-1.7.1_sr4.1-34.1
java-1_7_1-ibm-alsa-1.7.1_sr4.1-34.1

160226 - CentOS 6 CESA-2017-0527 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS 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:
CESA-2017-0527

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/022342.html

CentOS 6
noarch
tomcat6-servlet-2.5-api-6.0.24-105.el6_8
tomcat6-javadoc-6.0.24-105.el6_8
tomcat6-6.0.24-105.el6_8
tomcat6-lib-6.0.24-105.el6_8
tomcat6-el-2.1-api-6.0.24-105.el6_8
tomcat6-webapps-6.0.24-105.el6_8
tomcat6-admin-webapps-6.0.24-105.el6_8
tomcat6-docs-webapp-6.0.24-105.el6_8
tomcat6-jsp-2.1-api-6.0.24-105.el6_8

163300 - Oracle Enterprise Linux ELSA-2017-0527 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise 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:
ELSA-2017-0527

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/006786.html

OEL6

x86_64
tomcat6-servlet-2.5-api-6.0.24-105.el6_8
tomcat6-javadoc-6.0.24-105.el6_8
tomcat6-6.0.24-105.el6_8
tomcat6-lib-6.0.24-105.el6_8
tomcat6-el-2.1-api-6.0.24-105.el6_8
tomcat6-webapps-6.0.24-105.el6_8
tomcat6-admin-webapps-6.0.24-105.el6_8
tomcat6-docs-webapp-6.0.24-105.el6_8
tomcat6-jsp-2.1-api-6.0.24-105.el6_8

i386
tomcat6-servlet-2.5-api-6.0.24-105.el6_8
tomcat6-javadoc-6.0.24-105.el6_8
tomcat6-6.0.24-105.el6_8
tomcat6-lib-6.0.24-105.el6_8
tomcat6-el-2.1-api-6.0.24-105.el6_8
tomcat6-webapps-6.0.24-105.el6_8
tomcat6-admin-webapps-6.0.24-105.el6_8
tomcat6-docs-webapp-6.0.24-105.el6_8
tomcat6-jsp-2.1-api-6.0.24-105.el6_8

175129 - Scientific Linux Security ERRATA Moderate: tomcat6 on SL6.x (noarch) (1703-8501)

Category: SSH Module -> NonIntrusive -> Scientific 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:
Security ERRATA Moderate: tomcat6 on SL6.x (noarch) (1703-8501)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1703&L=scientific-linux-errata&F=&S=&P=8501

SL6
noarch
tomcat6-servlet-2.5-api-6.0.24-105.el6_8
tomcat6-javadoc-6.0.24-105.el6_8
tomcat6-6.0.24-105.el6_8
tomcat6-lib-6.0.24-105.el6_8
tomcat6-el-2.1-api-6.0.24-105.el6_8
tomcat6-webapps-6.0.24-105.el6_8
tomcat6-admin-webapps-6.0.24-105.el6_8
tomcat6-docs-webapp-6.0.24-105.el6_8
tomcat6-jsp-2.1-api-6.0.24-105.el6_8

178413 - Gentoo Linux GLSA-201703-03 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6542

Description

The scan detected that the host is missing the following update:
GLSA-201703-03

Observation

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

https://security.gentoo.org/glsa/201703-03

Affected packages:
net-misc/putty < 0.68

182307 - FreeBSD mysql Denial Of Service Vulnerability (7c27192f-0bc3-11e7-9940-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2017-3302

Description

The scan detected that the host is missing the following update:
mysql -- denial of service vulnerability (7c27192f-0bc3-11e7-9940-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/7c27192f-0bc3-11e7-9940-b499baebfeaf.html

Affected packages:
mariadb55-client <= 5.5.54
mariadb100-client < 10.0.30
mariadb101-client < 10.1.22
mysql55-client <= 5.5.54
mysql56-client < 5.6.21
mysql57-client < 5.7.5

182313 - FreeBSD drupal8 Multiple Vulnerabilities (2730c668-0b1c-11e7-8d52-6cf0497db129)

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

Risk Level: Medium

CVE: CVE-2017-6377, CVE-2017-6379, CVE-2017-6381

Description

The scan detected that the host is missing the following update:
drupal8 -- multiple vulnerabilities (2730c668-0b1c-11e7-8d52-6cf0497db129)

Observation

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

http://www.vuxml.org/freebsd/2730c668-0b1c-11e7-8d52-6cf0497db129.html

Affected packages:
drupal8 < 8.2.7

185628 - Ubuntu Linux 12.04, 14.04 USN-3183-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7444, CVE-2016-8610, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337

Description

The scan detected that the host is missing the following update:
USN-3183-2

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/003781.html

Ubuntu 12.04

libgnutls26_2.12.14-5ubuntu3.14

Ubuntu 14.04

libgnutls26_2.12.23-12ubuntu2.7

21316 - IBM WebSphere Message Broker Clicking Action Hijack Vulnerability (swg21997906)

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

Risk Level: Medium

CVE: CVE-2016-9010

Description

A vulnerability is present in some versions of IBM WebSphere Message Broker.

Observation

IBM WebSphere Message Broker is a popular advanced Enterprise Service Bus.

A vulnerability is present in some versions of IBM WebSphere Message Broker. The flaw lies in the WEBUI component. Successful exploitation could allow a remote attacker to hijack the clicking action of a user. To exploit this vulnerability, the victim must be persuaded to visit a malicious site.

21318 - IBM WebSphere MQ Information Disclosure Vulnerability (swg21998660)

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

Risk Level: Medium

CVE: CVE-2016-3052

Description

An information disclosure vulnerability is present in some versions of IBM WebSphere MQ.

Observation

IBM WebSphere MQ is a messaging solution.

An information disclosure vulnerability is present in some versions of IBM WebSphere MQ. The flaw consists in a specific configuration setting not causing the desired behavior. Successful exploitation could allow a malicious remote user to obtain highly sensitive information.

21319 - IBM WebSphere MQ Denial-Of-Service Vulnerability (swg21998661)

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

Risk Level: Medium

CVE: CVE-2016-3013

Description

A denial-of-service vulnerability is present in some versions of IBM WebSphere MQ.

Observation

IBM WebSphere MQ is a messaging solution.

A denial-of-service vulnerability is present in some versions of IBM WebSphere MQ. The flaw lies in the Message Channel Agent. Successful exploitation could allow an authenticated user to crash the MQ channel.

21320 - IBM WebSphere MQ Denial-Of-Service (swg21998647)

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

Risk Level: Medium

CVE: CVE-2016-9009

Description

A denial-of-service vulnerability is present in some versions of IBM WebSphere MQ.

Observation

IBM WebSphere MQ is a messaging solution.

A denial-of-service vulnerability is present in some versions of IBM WebSphere MQ. The flaw lies in the MQ clustering components. Successful exploitation could allow an authenticated user to cause a denial-of-service. Exploitation of this vulnerability requires the authenticated user to have the right permissions to create clusters.

21491 - IBM DB2 Information Disclosure Vulnerability Prior To 10.1 Fix Pack 6

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2017-1150

Description

A vulnerability is present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

A vulnerability is present in some versions of IBM DB2. The flaw is due to failure to update the user authorization cache when a table is renamed and a new table is created with the old name. Successful exploitation could allow an attacker to incorrectly acquire privileges to access the new table.

21541 - (SB10188) McAfee Threat Intelligence Exchange Server Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-7055, CVE-2017-3732

Description

Multiple vulnerabilities are present in some versions of McAfee Threat Intelligence Exchange Server.

Observation

McAfee Threat Intelligence Exchange Server is a real-time threat detection and response software.

Multiple vulnerabilities are present in some versions of McAfee Threat Intelligence Exchange Server. The flaws lie in the OpenSSL component. Successful exploitation could allow an attacker to disclose information or cause a denial of service condition.

185629 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3173-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8826

Description

The scan detected that the host is missing the following update:
USN-3173-2

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/003784.html

Ubuntu 16.04

nvidia-375_375.39-0ubuntu0.16.04.1
nvidia-367_375.39-0ubuntu0.16.04.1

Ubuntu 14.04

nvidia-367_375.39-0ubuntu0.14.04.1
nvidia-375_375.39-0ubuntu0.14.04.1

Ubuntu 16.10

nvidia-367_375.39-0ubuntu0.16.10.1
nvidia-375_375.39-0ubuntu0.16.10.1

185631 - Ubuntu Linux 14.04 USN-3234-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10208, CVE-2017-5551

Description

The scan detected that the host is missing the following update:
USN-3234-2

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/003779.html

Ubuntu 14.04

linux-image-powerpc64-emb-lts-xenial_4.4.0.67.54
linux-image-4.4.0-67-powerpc-smp_4.4.0-67.88~14.04.1
linux-image-4.4.0-67-generic_4.4.0-67.88~14.04.1
linux-image-4.4.0-67-powerpc-e500mc_4.4.0-67.88~14.04.1
linux-image-generic-lts-xenial_4.4.0.67.54
linux-image-4.4.0-67-powerpc64-emb_4.4.0-67.88~14.04.1
linux-image-powerpc-e500mc-lts-xenial_4.4.0.67.54
linux-image-4.4.0-67-lowlatency_4.4.0-67.88~14.04.1
linux-image-lowlatency-lts-xenial_4.4.0.67.54
linux-image-4.4.0-67-generic-lpae_4.4.0-67.88~14.04.1
linux-image-generic-lpae-lts-xenial_4.4.0.67.54
linux-image-4.4.0-67-powerpc64-smp_4.4.0-67.88~14.04.1
linux-image-powerpc-smp-lts-xenial_4.4.0.67.54
linux-image-powerpc64-smp-lts-xenial_4.4.0.67.54

185633 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3240-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-0318

Description

The scan detected that the host is missing the following update:
USN-3240-1

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/003785.html

Ubuntu 12.04

nvidia-331_340.102-0ubuntu0.12.04.1
nvidia-304_304.135-0ubuntu0.12.04.1
nvidia-340-updates_340.102-0ubuntu0.12.04.1
nvidia-current_304.135-0ubuntu0.12.04.1
nvidia-340_340.102-0ubuntu0.12.04.1
nvidia-331-updates_340.102-0ubuntu0.12.04.1
nvidia-304-updates_304.135-0ubuntu0.12.04.1

Ubuntu 16.04

nvidia-current_304.135-0ubuntu0.16.04.1
nvidia-331-updates_340.102-0ubuntu0.16.04.1
nvidia-375_375.39-0ubuntu0.16.04.1
nvidia-367_375.39-0ubuntu0.16.04.1
nvidia-304_304.135-0ubuntu0.16.04.1
nvidia-340_340.102-0ubuntu0.16.04.1

nvidia-340-updates_340.102-0ubuntu0.16.04.1
nvidia-304-updates_304.135-0ubuntu0.16.04.1
nvidia-331_340.102-0ubuntu0.16.04.1

Ubuntu 14.04

nvidia-340-updates_340.102-0ubuntu0.14.04.1
nvidia-375_375.39-0ubuntu0.14.04.1
nvidia-current_304.135-0ubuntu0.14.04.1
nvidia-304-updates_304.135-0ubuntu0.14.04.1
nvidia-331_340.102-0ubuntu0.14.04.1
nvidia-340_340.102-0ubuntu0.14.04.1
nvidia-304_304.135-0ubuntu0.14.04.1
nvidia-331-updates_340.102-0ubuntu0.14.04.1
nvidia-367_375.39-0ubuntu0.14.04.1

Ubuntu 16.10

nvidia-367_375.39-0ubuntu0.16.10.1
nvidia-current_304.135-0ubuntu0.16.10.1
nvidia-304_304.135-0ubuntu0.16.10.1
nvidia-340_340.102-0ubuntu0.16.10.1
nvidia-304-updates_304.135-0ubuntu0.16.10.1
nvidia-375_375.39-0ubuntu0.16.10.1
nvidia-331-updates_340.102-0ubuntu0.16.10.1
nvidia-340-updates_340.102-0ubuntu0.16.10.1
nvidia-331_340.102-0ubuntu0.16.10.1

185636 - Ubuntu Linux 16.04 USN-3234-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10208, CVE-2017-5551

Description

The scan detected that the host is missing the following update:
USN-3234-1

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/003778.html

Ubuntu 16.04

linux-image-4.4.0-1051-snapdragon_4.4.0-1051.55
linux-image-4.4.0-67-lowlatency_4.4.0-67.88
linux-image-powerpc64-emb_4.4.0.67.72
linux-image-4.4.0-1048-raspi2_4.4.0-1048.55
linux-image-4.4.0-67-powerpc-e500mc_4.4.0-67.88
linux-image-4.4.0-1006-gke_4.4.0-1006.6
linux-image-lowlatency_4.4.0.67.72
linux-image-gke_4.4.0.1006.7
linux-image-snapdragon_4.4.0.1051.44
linux-image-4.4.0-67-generic_4.4.0-67.88
linux-image-powerpc-smp_4.4.0.67.72
linux-image-4.4.0-67-generic-lpae_4.4.0-67.88

linux-image-4.4.0-67-powerpc-smp_4.4.0-67.88
linux-image-4.4.0-67-powerpc64-emb_4.4.0-67.88
linux-image-aws_4.4.0.1009.11
linux-image-4.4.0-1009-aws_4.4.0-1009.18
linux-image-powerpc-e500mc_4.4.0.67.72
linux-image-4.4.0-67-powerpc64-smp_4.4.0-67.88
linux-image-powerpc64-smp_4.4.0.67.72
linux-image-raspi2_4.4.0.1048.48
linux-image-generic-lpae_4.4.0.67.72
linux-image-generic_4.4.0.67.72

191841 - Fedora Linux 24 FEDORA-2017-2258cfb450 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6430

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2258cfb450

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=3

Fedora Core 24

ettercap-0.8.2-4.1.fc24

191844 - Fedora Linux 25 FEDORA-2017-0e9ad12958 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-2017-0e9ad12958

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=2

Fedora Core 25

icoutils-0.31.2-1.fc25

191852 - Fedora Linux 24 FEDORA-2017-e8460ebed6 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-e8460ebed6

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=2

Fedora Core 24

icoutils-0.31.2-1.fc24

191857 - Fedora Linux 25 FEDORA-2017-31b976672b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10155, CVE-2016-7907, CVE-2017-2615, CVE-2017-2620, CVE-2017-5525, CVE-2017-5526, CVE-2017-5552, CVE-2017-5578, CVE-2017-5667, CVE-2017-5856, CVE-2017-5857, CVE-2017-5898, CVE-2017-5987, CVE-2017-6058, CVE-2017-6505

Description

The scan detected that the host is missing the following update:
FEDORA-2017-31b976672b

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=2

Fedora Core 25

qemu-2.7.1-4.fc25

191859 - Fedora Linux 24 FEDORA-2017-62ac1230f7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10155, CVE-2017-2615, CVE-2017-2620, CVE-2017-5525, CVE-2017-5526, CVE-2017-5552, CVE-2017-5667, CVE-2017-5856, CVE-2017-5857, CVE-2017-5898, CVE-2017-5987, CVE-2017-6505

Description

The scan detected that the host is missing the following update:
FEDORA-2017-62ac1230f7

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

qemu-2.6.2-7.fc24

191860 - Fedora Linux 25 FEDORA-2017-b59943dcae Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
FEDORA-2017-b59943dcae

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=2

Fedora Core 25

qbittorrent-3.3.11-1.fc25

21326 - (K12685114) F5 BIG-IP BIG-IP REST Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2016-6249

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the REST Framework Logging component. Successful exploitation could allow local users to obtain sensitive information.

21344 - Novell eDirectory Multiple Vulnerabilities Prior To 9.0.2 Hot Fix 2

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Low

CVE: CVE-2017-5186

Description

Multiple vulnerabilities are present in some versions of Novell (NetIQ) eDirectory.

Observation

Novell (NetIQ) eDirectory is an X.500 compatible directory service software for centrally managing access to network resources.

Multiple vulnerabilities are present in some versions of Novell (NetIQ) eDirectory. The flaws lie in multiple components. Successful exploitation could allow a malicious user to cause a denial-of-service or other unspecified impact.

21504 - (SB10184) McAfee ePolicy Orchestrator Cross-Site Scripting Vulnerability

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

Risk Level: Low

CVE: CVE-2017-3902

Description

A cross-site scripting vulnerability is present in some versions of McAfee ePolicy Orchestrator.

Observation

McAfee ePolicy Orchestrator (ePO) is widely acknowledged as the most advanced and scalable security management software.

A cross-site scripting vulnerability is present in some versions of McAfee ePolicy Orchestrator. The flaw lies in the web interface. Successful exploitation could allow a remote attacker to execute arbitrary code.

88851 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-074-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2640

Description

The scan detected that the host is missing the following update:
SSA:2017-074-01

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.539975

Slackware 14.0
x86_64
pidgin-2.12.0-x86_64-1

Slackware 13.37
x86_64
pidgin-2.12.0-x86_64-1

Slackware 14.1
x86_64
pidgin-2.12.0-x86_64-1

Slackware 13.1
x86_64
pidgin-2.12.0-x86_64-1

Slackware 14.2
x86_64
pidgin-2.12.0-x86_64-1

i586
pidgin-2.12.0-i586-1

Slackware 13.0

x86_64
pidgin-2.12.0-x86_64-1

130722 - Debian Linux 8.0 DSA-3810-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-5029, CVE-2017-5030, CVE-2017-5031, CVE-2017-5032, CVE-2017-5033, CVE-2017-5034, CVE-2017-5035, CVE-2017-5036, CVE-2017-5037, CVE-2017-5038, CVE-2017-5039, CVE-2017-5040, CVE-2017-5041, CVE-2017-5042, CVE-2017-5043, CVE-2017-5044, CVE-2017-5045, CVE-2017-5046

Description

The scan detected that the host is missing the following update:
DSA-3810-1

Observation

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

http://www.debian.org/security/2017/dsa-3810

Debian 8.0
all
chromium-dbg_57.0.2987.98-1~deb8u1
chromedriver_57.0.2987.98-1~deb8u1
chromium-l10n_57.0.2987.98-1~deb8u1
chromium-inspector_57.0.2987.98-1~deb8u1
chromium_57.0.2987.98-1~deb8u1

130724 - Debian Linux 8.0 DSA-3812-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-6903

Description

The scan detected that the host is missing the following update:
DSA-3812-1

Observation

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

http://www.debian.org/security/2017/dsa-3812

Debian 8.0
all
ioquake3_1.36+u20140802+gca9eebb-2+deb8u1

145265 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0695-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:0695-1

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/002694.html

SuSE SLED 12 SP1
x86_64
dbus-1-x11-1.8.22-24.8.1
dbus-1-debuginfo-1.8.22-24.8.1
libdbus-1-3-1.8.22-24.8.1
libdbus-1-3-debuginfo-1.8.22-24.8.1
dbus-1-debuginfo-32bit-1.8.22-24.8.1
dbus-1-x11-debugsource-1.8.22-24.8.1
libdbus-1-3-32bit-1.8.22-24.8.1
libdbus-1-3-debuginfo-32bit-1.8.22-24.8.1
dbus-1-1.8.22-24.8.1
dbus-1-x11-debuginfo-1.8.22-24.8.1
dbus-1-debugsource-1.8.22-24.8.1

SuSE SLES 12 SP2
x86_64
dbus-1-x11-1.8.22-24.8.1
dbus-1-debuginfo-1.8.22-24.8.1
libdbus-1-3-1.8.22-24.8.1
libdbus-1-3-debuginfo-1.8.22-24.8.1
dbus-1-debuginfo-32bit-1.8.22-24.8.1
dbus-1-x11-debugsource-1.8.22-24.8.1
libdbus-1-3-32bit-1.8.22-24.8.1
libdbus-1-3-debuginfo-32bit-1.8.22-24.8.1
dbus-1-1.8.22-24.8.1
dbus-1-x11-debuginfo-1.8.22-24.8.1
dbus-1-debugsource-1.8.22-24.8.1

SuSE SLED 12 SP2
x86_64
dbus-1-x11-1.8.22-24.8.1
dbus-1-debuginfo-1.8.22-24.8.1
libdbus-1-3-1.8.22-24.8.1
libdbus-1-3-debuginfo-1.8.22-24.8.1
dbus-1-debuginfo-32bit-1.8.22-24.8.1
dbus-1-x11-debugsource-1.8.22-24.8.1
libdbus-1-3-32bit-1.8.22-24.8.1
libdbus-1-3-debuginfo-32bit-1.8.22-24.8.1
dbus-1-1.8.22-24.8.1
dbus-1-x11-debuginfo-1.8.22-24.8.1
dbus-1-debugsource-1.8.22-24.8.1

SuSE SLES 12 SP1
x86_64
dbus-1-x11-1.8.22-24.8.1
dbus-1-debuginfo-1.8.22-24.8.1
libdbus-1-3-1.8.22-24.8.1
libdbus-1-3-debuginfo-1.8.22-24.8.1
dbus-1-debuginfo-32bit-1.8.22-24.8.1

dbus-1-x11-debugsource-1.8.22-24.8.1
libdbus-1-3-32bit-1.8.22-24.8.1
libdbus-1-3-debuginfo-32bit-1.8.22-24.8.1
dbus-1-1.8.22-24.8.1
dbus-1-x11-debuginfo-1.8.22-24.8.1
dbus-1-debugsource-1.8.22-24.8.1

182306 - FreeBSD firefox Integer Overflow In CreateImageBitmap () (5f453b69-abab-4e76-b6e5-2ed0bafcaee3)

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

Risk Level: Low

CVE: CVE-2017-5428

Description

The scan detected that the host is missing the following update:
firefox -- integer overflow in createImageBitmap() (5f453b69-abab-4e76-b6e5-2ed0bafcaee3)

Observation

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

http://www.vuxml.org/freebsd/5f453b69-abab-4e76-b6e5-2ed0bafcaee3.html

Affected packages:
firefox < 52.0.1,1

182308 - FreeBSD irssi Use-after-free Potential Code Execution (06f931c0-0be0-11e7-b4bf-5404a68ad561)

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:
irssi -- use-after-free potential code execution (06f931c0-0be0-11e7-b4bf-5404a68ad561)

Observation

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

http://www.vuxml.org/freebsd/06f931c0-0be0-11e7-b4bf-5404a68ad561.html

Affected packages:
0.8.21,1 < irssi < 1.0.2,1

182310 - FreeBSD PuTTY Integer Overflow Permits Memory Overwrite By Forwarded Ssh-agent Connections (9b973e97-0a99-11e7-ace7-080027ef73ec

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

Risk Level: Low

CVE: CVE-2017-6542

Description

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

PuTTY -- integer overflow permits memory overwrite by forwarded ssh-agent connections (9b973e97-0a99-11e7-ace7-080027ef73ec)

Observation

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

http://www.vuxml.org/freebsd/9b973e97-0a99-11e7-ace7-080027ef73ec.html

Affected packages:
putty < 0.68

182311 - FreeBSD moodle Multiple Vulnerabilities (df45b4bd-0b7f-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:
moodle -- multiple vulnerabilities (df45b4bd-0b7f-11e7-970f-002590263bf5)

Observation

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

http://www.vuxml.org/freebsd/df45b4bd-0b7f-11e7-970f-002590263bf5.html

Affected packages:
moodle29 <= 2.9.9
moodle30 < 3.0.9
moodle31 < 3.1.5
moodle32 < 3.2.2

185634 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3238-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-5428

Description

The scan detected that the host is missing the following update:
USN-3238-1

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/003783.html

Ubuntu 12.04

firefox_52.0.1+build2-0ubuntu0.12.04.1

Ubuntu 16.04

firefox_52.0.1+build2-0ubuntu0.16.04.1

Ubuntu 14.04

firefox_52.0.1+build2-0ubuntu0.14.04.1

Ubuntu 16.10

firefox_52.0.1+build2-0ubuntu0.16.10.1

191842 - Fedora Linux 24 FEDORA-2017-9d06448c3e 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-2017-9d06448c3e

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

knot-resolver-1.2.4-1.fc24

191843 - Fedora Linux 24 FEDORA-2017-788129b61c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2623

Description

The scan detected that the host is missing the following update:
FEDORA-2017-788129b61c

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

rpm-ostree-2017.3-2.fc24

191846 - Fedora Linux 24 FEDORA-2017-c1bec8972c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8654, CVE-2016-9262

Description

The scan detected that the host is missing the following update:
FEDORA-2017-c1bec8972c

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

jasper-1.900.13-3.fc24

191848 - Fedora Linux 25 FEDORA-2017-19b5c9f1c6 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-2017-19b5c9f1c6

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=2

Fedora Core 25

sscg-2.0.3-1.fc25

191849 - Fedora Linux 25 FEDORA-2017-d215a25e41 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-d215a25e41

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=2

Fedora Core 25

wordpress-4.7.3-1.fc25

191850 - Fedora Linux 24 FEDORA-2017-7e0b84ffad 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-2017-7e0b84ffad

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=2

Fedora Core 24

wordpress-4.7.3-1.fc24

191853 - Fedora Linux 25 FEDORA-2017-df53d02da7 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-df53d02da7

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

knot-resolver-1.2.4-1.fc25

191854 - Fedora Linux 25 FEDORA-2017-003fa5648c Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-2623

Description

The scan detected that the host is missing the following update:
FEDORA-2017-003fa5648c

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

rpm-ostree-2017.3-2.fc25

191856 - Fedora Linux 24 FEDORA-2017-6558bc25bc 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-2017-6558bc25bc

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=2

Fedora Core 24

sscg-2.0.3-1.fc24

191858 - Fedora Linux 25 FEDORA-2017-3dba8a70ce Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8654, CVE-2016-9262

Description

The scan detected that the host is missing the following update:
FEDORA-2017-3dba8a70ce

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=2

Fedora Core 25

jasper-1.900.13-3.fc25

191861 - Fedora Linux 26 FEDORA-2017-83671c0fa0 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-2017-83671c0fa0

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 26

cloud-init-0.7.9-4.fc26

191862 - Fedora Linux 24 FEDORA-2017-ce66f11df1 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-ce66f11df1

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=3

Fedora Core 24

deluge-1.3.14-1.fc24

141520 - Red Hat Enterprise Linux RHSA-2017-0621 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-3712

Description

The scan detected that the host is missing the following update:
RHSA-2017-0621

Observation

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

https://rhn.redhat.com/errata/RHSA-2017-0621.html

RHEL6D
x86_64
qemu-kvm-tools-0.12.1.2-2.503.el6
qemu-guest-agent-0.12.1.2-2.503.el6
qemu-img-0.12.1.2-2.503.el6
qemu-kvm-0.12.1.2-2.503.el6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6

i386
qemu-guest-agent-0.12.1.2-2.503.el6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6

RHEL6S
i386
qemu-guest-agent-0.12.1.2-2.503.el6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6

x86_64
qemu-kvm-tools-0.12.1.2-2.503.el6
qemu-guest-agent-0.12.1.2-2.503.el6
qemu-img-0.12.1.2-2.503.el6
qemu-kvm-0.12.1.2-2.503.el6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6

RHEL6WS
x86_64
qemu-kvm-tools-0.12.1.2-2.503.el6
qemu-guest-agent-0.12.1.2-2.503.el6
qemu-img-0.12.1.2-2.503.el6
qemu-kvm-0.12.1.2-2.503.el6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6

i386
qemu-guest-agent-0.12.1.2-2.503.el6
qemu-kvm-debuginfo-0.12.1.2-2.503.el6

191840 - Fedora Linux 25 FEDORA-2017-3d16d348eb Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9603, CVE-2017-6505

Description

The scan detected that the host is missing the following update:
FEDORA-2017-3d16d348eb

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

xen-4.7.2-2.fc25

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.

21104 - (K03151140) F5 BIG-IP Imagemagick Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-3714

Update Details

FASLScript is updated

21409 - (MS17-018) Security Update for Windows Kernel-Mode Drivers (4013083)

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

Risk Level: High

CVE: CVE-2017-0024, CVE-2017-0026, CVE-2017-0056, CVE-2017-0078, CVE-2017-0079, CVE-2017-0080, CVE-2017-0081, CVE-2017-0082

Update Details

Risk is updated

21481 - (MS17-008) Security Update for Windows Hyper-V (4013082)

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

Risk Level: High

CVE: CVE-2017-0021, CVE-2017-0051, CVE-2017-0074, CVE-2017-0075, CVE-2017-0076, CVE-2017-0095, CVE-2017-0096, CVE-2017-0097, CVE-2017-0098, CVE-2017-0099, CVE-2017-0109

Update Details

Risk is updated

130683 - Debian Linux 8.0 DSA-3766-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5522

Update Details

Risk is updated

130702 - Debian Linux 8.0 DSA-3789-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10195, CVE-2016-10196, CVE-2016-10197

Update Details

Risk is updated

181437 - FreeBSD tomcat Multiple Vulnerabilities (25e0593d-13c0-11e5-9afb-3c970e169bc2)

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

Risk Level: High

CVE: CVE-2014-0230, CVE-2014-7810

Update Details

FASLScript is updated

182023 - FreeBSD Apache Commons FileUpload Denial Of Service (61b8c359-4aab-11e6-a7bd-14dae9d210b8)

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

Risk Level: High

CVE: CVE-2016-3092

Update Details

FASLScript is updated

185486 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3131-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8354, CVE-2014-8355, CVE-2014-8562, CVE-2014-8716, CVE-2014-9805, CVE-2014-9806, CVE-2014-9807, CVE-2014-9808, CVE-2014-9809, CVE-2014-9810, CVE-2014-9811, CVE-2014-9812, CVE-2014-9813, CVE-2014-9814, CVE-2014-9815, CVE-2014-9816, CVE-2014-9817, CVE-2014-9818, CVE-2014-9819, CVE-2014-9820, CVE-2014-9821, CVE-2014-9822, CVE-2014-9823, CVE-2014-9826, CVE-2014-9828, CVE-2014-9829, CVE-2014-9830, CVE-2014-9831, CVE-2014-9833, CVE-2014-9834, CVE-2014-9835, CVE-2014-9836, CVE-2014-9837, CVE-2014-9838, CVE-2014-9839, CVE-2014-9840, CVE-2014-9841, CVE-2014-9843, CVE-2014-9844, CVE-2014-9845

Update Details

Risk is updated

185625 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3228-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10195, CVE-2016-10196, CVE-2016-10197

Update Details

Risk is updated

191667 - Fedora Linux 25 FEDORA-2017-93ed1d1687 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5522

Update Details

Risk is updated

21210 - (MS17-017) Security Update for Windows Kernel (4013081)

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

Risk Level: Medium

CVE: CVE-2017-0050, CVE-2017-0101, CVE-2017-0102, CVE-2017-0103

Update Details

Risk is updated

181863 - FreeBSD tomcat Multiple Vulnerabilities (1f1124fe-de5c-11e5-8fa8-14dae9d210b8)

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

Risk Level: Medium

CVE: CVE-2015-5345, CVE-2015-5346, CVE-2016-0706, CVE-2016-0714

Update Details

FASLScript is updated

16834 - (K12636) F5 BIG-IP Slowloris Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2007-6750

Update Details

FASLScript is updated

21079 - (K35155453) F5 BIG-IP Multiple LibTIFF Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2014-8127, CVE-2014-8129, CVE-2014-8130, CVE-2014-9655, CVE-2015-8665, CVE-2015-8683, CVE-2015-8781, CVE-2015-8782, CVE-2015-8783

Update Details

FASLScript is updated

21270 - (K50116122) F5 BIG-IP Apache Tomcat Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-6816

Update Details

FASLScript is updated

181232 - FreeBSD tomcat Multiple Vulnerabilities (81fc1076-1286-11e4-bebd-000c2980a9f3)

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

Risk Level: Medium

CVE: CVE-2014-0075, CVE-2014-0096, CVE-2014-0099

Update Details

FASLScript is updated

21078 - (K89096577) F5 BIG-IP LibTIFF Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-8784, CVE-2016-5320

Update Details

FASLScript is updated

130695 - Debian Linux 8.0 DSA-3784-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5938

Update Details

Risk is updated

130719 - Debian Linux 8.0 DSA-3808-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10252, CVE-2017-6498, CVE-2017-6499, CVE-2017-6500

Update Details

CVE is updated

178370 - Gentoo Linux GLSA-201701-73 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4645, CVE-2015-4646

Update Details

Risk is updated

178397 - Gentoo Linux GLSA-201702-28 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10155, CVE-2017-2615, CVE-2017-5525, CVE-2017-5552, CVE-2017-5578, CVE-2017-5579, CVE-2017-5667, CVE-2017-5856, CVE-2017-5857, CVE-2017-5898, CVE-2017-5931

Update Details

Risk is updated

189524 - Fedora Linux 22 FEDORA-2015-10750 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4645, CVE-2015-4646

Update Details

Risk is updated

189558 - Fedora Linux 21 FEDORA-2015-10760 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-4645, CVE-2015-4646

Update Details
Risk is updated

191680 - Fedora Linux 25 FEDORA-2017-07d308fd81 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-10187

Update Details
Risk is updated

191701 - Fedora Linux 24 FEDORA-2017-efed73a87c Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-10187

Update Details
Risk is updated

191703 - Fedora Linux 25 FEDORA-2017-1855c8af2c Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-2586, CVE-2017-2587, CVE-2017-5849

Update Details
Risk is updated

191785 - Fedora Linux 24 FEDORA-2017-fa4e441e03 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-2586, CVE-2017-2587, CVE-2017-5849

Update Details
Risk is updated

191792 - Fedora Linux 25 FEDORA-2017-5a6ed9d326 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-6414

Update Details

Risk is updated

191821 - Fedora Linux 25 FEDORA-2017-06365bdcfd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-6430

Update Details

Risk is updated

83905 - FreeBSD tomcat Multiple Vulnerabilities (f599dfc4-3ec2-11e2-8ae1-001a8056d0b5)

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

Risk Level: Low

CVE: CVE-2012-3546, CVE-2012-4431, CVE-2012-4534

Update Details

FASLScript is updated

83912 - FreeBSD tomcat Bypass Of CSRF Prevention Filter (953911fe-51ef-11e2-8e34-0022156e8794)

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

Risk Level: Low

CVE: CVE-2012-4431

Update Details

FASLScript is updated

83918 - FreeBSD tomcat Denial Of Service (134acaa2-51ef-11e2-8e34-0022156e8794)

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

Risk Level: Low

CVE: CVE-2012-4534

Update Details

FASLScript is updated

182242 - FreeBSD tomcat Multiple Vulnerabilities (3ae106e2-d521-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-0762, CVE-2016-5018, CVE-2016-6794, CVE-2016-6796, CVE-2016-6797

Update Details

FASLScript is updated

182244 - FreeBSD tomcat Multiple Vulnerabilities (0b9af110-d529-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-6816, CVE-2016-8735

Update Details

FASLScript is updated

182253 - FreeBSD tomcat Information Disclosure Vulnerability (e5ec2767-d529-11e6-ae1b-002590263bf5)

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

Risk Level: Low

CVE: CVE-2016-8745

Update Details

FASLScript is updated

70014 - netbios-helpers.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70103 - novell.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70131 - f5.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.