2016-DEC-01
FSL version 7.5.868

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

20913 - Apache Tomcat Multiple Vulnerabilities Prior To 9.0.0.M13

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

Risk Level: High

CVE: CVE-2016-3427, CVE-2016-6816, CVE-2016-6817, CVE-2016-8735

Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws lie in several components. Successful exploitation could allow an attacker to obtain sensitive information, cause a denial of service or execute arbitrary code.

20914 - Apache Tomcat Multiple Vulnerabilities Prior To 7.0.73

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

Risk Level: High

CVE: CVE-2016-3427, CVE-2016-6816, CVE-2016-8735

Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws lie in several components. Successful exploitation could allow an attacker to obtain sensitive information, execute arbitrary code.

20915 - Apache Tomcat Multiple Vulnerabilities Prior To 6.0.48

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

Risk Level: High

CVE: CVE-2016-3427, CVE-2016-6816, CVE-2016-8735

Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

Observation

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws lie in several components. Successful exploitation could allow an attacker to obtain sensitive information or execute arbitrary code.

20925 - Apache Tomcat Multiple Vulnerabilities Prior To 8.5.8

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

Risk Level: High

CVE: CVE-2016-6816, CVE-2016-6817, CVE-2016-8735

Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

Observation

Apache Tomcat is a Java application server.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information, cause denial of service condition or execute arbitrary code.

20926 - (SOL22334603) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-0799, CVE-2016-2842

Description

Multiple vulnerabilities are 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.

Multiple vulnerabilities are present in some versions of F5 BIG-IP products. The flaws lie in the OpenSSL Component. Successful exploitation could allow an attacker to cause a denial of service condition or possibly have other unspecified impact in the target system.

130640 - Debian Linux 8.0 DSA-3725-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9911, CVE-2015-2632, CVE-2015-4844, CVE-2016-0494, CVE-2016-6293, CVE-2016-7415

Description

The scan detected that the host is missing the following update:
DSA-3725-1

Observation

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

http://www.debian.org/security/2016/dsa-3725

Debian 8.0
all
icu-devtools_52.1-8+deb8u4

libicu52-dbg_52.1-8+deb8u4
icu-doc_52.1-8+deb8u4
libicu-dev_52.1-8+deb8u4
libicu52_52.1-8+deb8u4

145027 - SuSE SLES 11 SP4 SUSE-SU-2016:2902-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7161, CVE-2016-7170, CVE-2016-7908, CVE-2016-7909, CVE-2016-8576, CVE-2016-8577, CVE-2016-8578, CVE-2016-8667, CVE-2016-8669, CVE-2016-8909, CVE-2016-8910, CVE-2016-9101, CVE-2016-9102, CVE-2016-9103, CVE-2016-9104, CVE-2016-9105, CVE-2016-9106

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2902-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002419.html

SuSE SLES 11 SP4
i586
kvm-1.4.2-50.1

x86_64
kvm-1.4.2-50.1

20911 - (SOL50118123) F5 BIG-IP Java Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-0466, CVE-2016-0483

Description

Multiple vulnerabilities are 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.

Multiple vulnerabilities are present in some versions of F5 BIG-IP products. The flaws lie in Oracle Java SE. Successful exploitation could allow an attacker to cause a denial of service condition or execute remote code.

20924 - IBM Tivoli Storage Manager FastBack Stack Based Buffer Overflow Elevation Of Privilege Vulnerability

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

Risk Level: High

CVE: CVE-2016-6091

Description

A buffer overflow vulnerability is present in some versions of IBM Tivoli Storage Manager FastBack.

Observation

IBM Tivoli Storage Manager FastBack is a data protection and recovery software.

A buffer overflow vulnerability is present in some versions of IBM Tivoli Storage Manager FastBack. The flaw lies in mount process. Successful exploitation could allow an attacker to cause application crash or execute arbitrary code.

145017 - SuSE Linux 13.2 openSUSE-SU-2016:2900-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5568, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2900-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-11/msg00108.html

SuSE Linux 13.2
i586
java-1_7_0-openjdk-1.7.0.121-28.2
java-1_7_0-openjdk-src-1.7.0.121-28.2
java-1_7_0-openjdk-bootstrap-1.7.0.121-28.2
java-1_7_0-openjdk-headless-debuginfo-1.7.0.121-28.2
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.121-28.2
java-1_7_0-openjdk-demo-1.7.0.121-28.2
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.121-28.2
java-1_7_0-openjdk-demo-debuginfo-1.7.0.121-28.2
java-1_7_0-openjdk-bootstrap-devel-1.7.0.121-28.2
java-1_7_0-openjdk-devel-debuginfo-1.7.0.121-28.2
java-1_7_0-openjdk-bootstrap-headless-1.7.0.121-28.2
java-1_7_0-openjdk-accessibility-1.7.0.121-28.2
java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.121-28.2
java-1_7_0-openjdk-debuginfo-1.7.0.121-28.2
java-1_7_0-openjdk-headless-1.7.0.121-28.2
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.121-28.2
java-1_7_0-openjdk-debugsource-1.7.0.121-28.2
java-1_7_0-openjdk-devel-1.7.0.121-28.2

noarch
java-1_7_0-openjdk-javadoc-1.7.0.121-28.2

x86_64
java-1_7_0-openjdk-1.7.0.121-28.2
java-1_7_0-openjdk-src-1.7.0.121-28.2
java-1_7_0-openjdk-bootstrap-1.7.0.121-28.2
java-1_7_0-openjdk-headless-debuginfo-1.7.0.121-28.2
java-1_7_0-openjdk-bootstrap-devel-debuginfo-1.7.0.121-28.2
java-1_7_0-openjdk-demo-1.7.0.121-28.2
java-1_7_0-openjdk-bootstrap-debugsource-1.7.0.121-28.2
java-1_7_0-openjdk-demo-debuginfo-1.7.0.121-28.2
java-1_7_0-openjdk-bootstrap-devel-1.7.0.121-28.2
java-1_7_0-openjdk-devel-debuginfo-1.7.0.121-28.2

java-1_7_0-openjdk-bootstrap-headless-1.7.0.121-28.2
java-1_7_0-openjdk-accessibility-1.7.0.121-28.2
java-1_7_0-openjdk-bootstrap-headless-debuginfo-1.7.0.121-28.2
java-1_7_0-openjdk-debuginfo-1.7.0.121-28.2
java-1_7_0-openjdk-headless-1.7.0.121-28.2
java-1_7_0-openjdk-bootstrap-debuginfo-1.7.0.121-28.2
java-1_7_0-openjdk-debugsource-1.7.0.121-28.2
java-1_7_0-openjdk-devel-1.7.0.121-28.2

145030 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2887-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5542, CVE-2016-5554, CVE-2016-5556, CVE-2016-5568, CVE-2016-5573, CVE-2016-5582, CVE-2016-5597

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2887-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002412.html

SuSE SLED 12 SP1
x86_64
java-1_8_0-openjdk-debugsource-1.8.0.111-17.1
java-1_8_0-openjdk-headless-1.8.0.111-17.1
java-1_8_0-openjdk-1.8.0.111-17.1
java-1_8_0-openjdk-debuginfo-1.8.0.111-17.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.111-17.1

SuSE SLES 12 SP2
x86_64
java-1_8_0-openjdk-devel-1.8.0.111-17.1
java-1_8_0-openjdk-headless-1.8.0.111-17.1
java-1_8_0-openjdk-demo-1.8.0.111-17.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.111-17.1
java-1_8_0-openjdk-devel-debuginfo-1.8.0.111-17.1
java-1_8_0-openjdk-debugsource-1.8.0.111-17.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.111-17.1
java-1_8_0-openjdk-1.8.0.111-17.1
java-1_8_0-openjdk-debuginfo-1.8.0.111-17.1

SuSE SLED 12 SP2
x86_64
java-1_8_0-openjdk-debugsource-1.8.0.111-17.1
java-1_8_0-openjdk-headless-1.8.0.111-17.1
java-1_8_0-openjdk-1.8.0.111-17.1
java-1_8_0-openjdk-debuginfo-1.8.0.111-17.1
java-1_8_0-openjdk-headless-debuginfo-1.8.0.111-17.1

SuSE SLES 12 SP1
x86_64
java-1_8_0-openjdk-devel-1.8.0.111-17.1
java-1_8_0-openjdk-headless-1.8.0.111-17.1
java-1_8_0-openjdk-demo-1.8.0.111-17.1

java-1_8_0-openjdk-headless-debuginfo-1.8.0.111-17.1
java-1_8_0-openjdk-debugsource-1.8.0.111-17.1
java-1_8_0-openjdk-demo-debuginfo-1.8.0.111-17.1
java-1_8_0-openjdk-1.8.0.111-17.1
java-1_8_0-openjdk-debuginfo-1.8.0.111-17.1

20903 - Mozilla Firefox Multiple Vulnerabilities Prior To 50

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

Risk Level: High

CVE: CVE-2016-5289, CVE-2016-5290, CVE-2016-5291, CVE-2016-5292, CVE-2016-5293, CVE-2016-5294, CVE-2016-5295, CVE-2016-5296, CVE-2016-5297, CVE-2016-5298, CVE-2016-5299, CVE-2016-9061, CVE-2016-9062, CVE-2016-9063, CVE-2016-9064, CVE-2016-9065, CVE-2016-9066, CVE-2016-9067, CVE-2016-9068, CVE-2016-9069, CVE-2016-9070, CVE-2016-9071, CVE-2016-9072, CVE-2016-9073, CVE-2016-9074, CVE-2016-9075, CVE-2016-9076, CVE-2016-9077

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

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

20904 - Mozilla Firefox Multiple Vulnerabilities Prior To 50

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-5289, CVE-2016-5290, CVE-2016-5291, CVE-2016-5292, CVE-2016-5293, CVE-2016-5294, CVE-2016-5295, CVE-2016-5296, CVE-2016-5297, CVE-2016-5298, CVE-2016-5299, CVE-2016-9061, CVE-2016-9062, CVE-2016-9063, CVE-2016-9064, CVE-2016-9065, CVE-2016-9066, CVE-2016-9067, CVE-2016-9068, CVE-2016-9069, CVE-2016-9070, CVE-2016-9071, CVE-2016-9072, CVE-2016-9073, CVE-2016-9074, CVE-2016-9075, CVE-2016-9076, CVE-2016-9077

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

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

20921 - (SYM16-021) Symantec Norton Client DLL Pre-Loading Uncontrolled Search Path Elevation of Privilege Vulnerability

Category: Windows Host Assessment -> Anti-Virus Software
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-5311

Description

A DLL loading privilege escalation vulnerability is present in the Norton Client in multiple Symantec products.

Observation

Symantec Norton Client is an endpint protection client present in multiple Symantec products.

A DLL loading privilege escalation vulnerability is present in the Norton Client in multiple Symantec products. The flaw is due to improper restrictions when system libraries are loaded. Successful exploitation could allow an attacker to cause a denial of service or execute arbitrary code with elevated privileges.

20884 - Novell Sentinel Vulnerability Prior To 7.3.4.0

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1000031

Description

A java deserialization vulnerability is present in some versions of NetIQ Sentinel.

Observation

NetIQ Sentinel is a SIEM software that provides monitoring and management on real-time.

A java deserialization vulnerability is present in some versions of NetIQ Sentinel. The flaw lies in the Apache Commons component. Successful exploitation could allow an attacker to remotely execute arbitrary code.

20907 - (SYM16-020) Symantec IT Management Suite DLL Loading Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2016-6590

Description

An arbitrary code execution vulnerability exists in some versions of Symantec ITMS.

Observation

Symantec ITMS is a network-based computer management solution.

An arbitrary code execution vulnerability exists in some versions of Symantec ITMS. The flaw lies in how this software handles the loading of DLL dependencies. Successful exploitation of this vulnerability could allow a malicious user to execute arbitrary code. Exploitation of this vulnerability requires a non-privileged user to click on a malicious URL within a website or an email.

20909 - (SYM16-020) Symantec Endpoint Virtualization DLL Loading Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2016-6590

Description

A vulnerability is present in some versions of Symantec Endpoint Encryption.

Observation

Symantec Endpoint Virtualization is a suite of products used for data storing in virtual layers.

A vulnerability is present in some versions of Symantec Endpoint Encryption. The flaw is due to DLL loading issues. Successful

exploitation could allow an attacker to execute arbitrary code.

20919 - (VMSA-2016-0022) VMware vCenter Server XML External Entity vulnerabilities

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

Risk Level: High

CVE: CVE-2016-7459, CVE-2016-7460

Description

Multiple vulnerabilities are present in some versions of VMware vCenter Server.

Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere.

Multiple vulnerabilities are present in some versions of VMware vCenter Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to disclose information or to cause a denial of service condition.

20920 - (VMSA-2016-0022) VMware vCenter Server XML External Entity vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-7459, CVE-2016-7460

Description

Multiple vulnerabilities are present in some versions of VMware vCenter Server.

Observation

VMware vCenter Server is a scalable and extensible platform to manage VMware vSphere.

Multiple vulnerabilities are present in some versions of VMware vCenter Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to disclose information or to cause a denial of service condition.

20928 - (CTX218775) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-9379, CVE-2016-9380, CVE-2016-9381, CVE-2016-9382, CVE-2016-9383, CVE-2016-9385, CVE-2016-9386

Description

Multiple vulnerabilities are present in some versions of Citrix XenServer.

Observation

Citrix XenServer is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of Citrix XenServer. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code on the host.

132307 - Oracle VM OVMSA-2016-0167 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8956, CVE-2016-1583, CVE-2016-3070, CVE-2016-4569, CVE-2016-4578, CVE-2016-6136, CVE-2016-6480

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0167

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-November/000592.html

OVM3.2
x86_64
kernel-uek-firmware-2.6.39-400.290.2.el5uek
kernel-uek-2.6.39-400.290.2.el5uek

132308 - Oracle VM OVMSA-2016-0168 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0718

Description

The scan detected that the host is missing the following update:
OVMSA-2016-0168

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2016-November/000594.html
http://oss.oracle.com/pipermail/oraclevm-errata/2016-November/000593.html

OVM3.3
x86_64
expat-2.0.1-13.el6_8

OVM3.4
x86_64
expat-2.0.1-13.el6_8

141371 - Red Hat Enterprise Linux RHSA-2016-2825 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5290

Description

The scan detected that the host is missing the following update:
RHSA-2016-2825

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2825.html

RHEL6S
i386
thunderbird-45.5.0-1.el6_8
thunderbird-debuginfo-45.5.0-1.el6_8

x86_64
thunderbird-45.5.0-1.el6_8
thunderbird-debuginfo-45.5.0-1.el6_8

RHEL6WS
x86_64
thunderbird-45.5.0-1.el6_8
thunderbird-debuginfo-45.5.0-1.el6_8

i386
thunderbird-45.5.0-1.el6_8
thunderbird-debuginfo-45.5.0-1.el6_8

RHEL5D
x86_64
thunderbird-debuginfo-45.5.0-1.el5_11
thunderbird-45.5.0-1.el5_11

i386
thunderbird-debuginfo-45.5.0-1.el5_11
thunderbird-45.5.0-1.el5_11

RHEL7D
x86_64
thunderbird-debuginfo-45.5.0-1.el7_3
thunderbird-45.5.0-1.el7_3

RHEL6D
x86_64
thunderbird-45.5.0-1.el6_8
thunderbird-debuginfo-45.5.0-1.el6_8

i386
thunderbird-45.5.0-1.el6_8
thunderbird-debuginfo-45.5.0-1.el6_8

RHEL7WS
x86_64
thunderbird-debuginfo-45.5.0-1.el7_3
thunderbird-45.5.0-1.el7_3

141372 - Red Hat Enterprise Linux RHSA-2016-2820 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8704, CVE-2016-8705

Description

The scan detected that the host is missing the following update:
RHSA-2016-2820

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2820.html

RHEL6S
i386
memcached-1.4.4-3.el6_8.1
memcached-devel-1.4.4-3.el6_8.1
memcached-debuginfo-1.4.4-3.el6_8.1

x86_64
memcached-1.4.4-3.el6_8.1
memcached-devel-1.4.4-3.el6_8.1
memcached-debuginfo-1.4.4-3.el6_8.1

RHEL6WS
x86_64
memcached-debuginfo-1.4.4-3.el6_8.1
memcached-1.4.4-3.el6_8.1

i386
memcached-debuginfo-1.4.4-3.el6_8.1
memcached-1.4.4-3.el6_8.1

RHEL6D
x86_64
memcached-1.4.4-3.el6_8.1
memcached-devel-1.4.4-3.el6_8.1
memcached-debuginfo-1.4.4-3.el6_8.1

i386
memcached-1.4.4-3.el6_8.1
memcached-devel-1.4.4-3.el6_8.1
memcached-debuginfo-1.4.4-3.el6_8.1

141373 - Red Hat Enterprise Linux RHSA-2016-2824 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0718

Description

The scan detected that the host is missing the following update:
RHSA-2016-2824

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2824.html

RHEL6S
i386
expat-debuginfo-2.0.1-13.el6_8
expat-2.0.1-13.el6_8
expat-devel-2.0.1-13.el6_8

x86_64
expat-debuginfo-2.0.1-13.el6_8
expat-2.0.1-13.el6_8
expat-devel-2.0.1-13.el6_8

RHEL6WS
x86_64
expat-debuginfo-2.0.1-13.el6_8
expat-2.0.1-13.el6_8
expat-devel-2.0.1-13.el6_8

i386
expat-debuginfo-2.0.1-13.el6_8
expat-2.0.1-13.el6_8
expat-devel-2.0.1-13.el6_8

RHEL7D
x86_64
expat-debuginfo-2.1.0-10.el7_3
expat-static-2.1.0-10.el7_3
expat-2.1.0-10.el7_3
expat-devel-2.1.0-10.el7_3

RHEL6D
x86_64
expat-debuginfo-2.0.1-13.el6_8
expat-2.0.1-13.el6_8
expat-devel-2.0.1-13.el6_8

i386
expat-debuginfo-2.0.1-13.el6_8
expat-2.0.1-13.el6_8
expat-devel-2.0.1-13.el6_8

RHEL7WS
x86_64
expat-debuginfo-2.1.0-10.el7_3
expat-static-2.1.0-10.el7_3
expat-2.1.0-10.el7_3
expat-devel-2.1.0-10.el7_3

141374 - Red Hat Enterprise Linux RHSA-2016-2819 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8704, CVE-2016-8705, CVE-2016-8706

Description

The scan detected that the host is missing the following update:
RHSA-2016-2819

Observation

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

https://rhn.redhat.com/errata/RHSA-2016-2819.html

RHEL7D
x86_64
memcached-debuginfo-1.4.15-10.el7_3.1
memcached-devel-1.4.15-10.el7_3.1
memcached-1.4.15-10.el7_3.1

RHEL7WS
x86_64
memcached-debuginfo-1.4.15-10.el7_3.1
memcached-devel-1.4.15-10.el7_3.1
memcached-1.4.15-10.el7_3.1

145019 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2912-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8956, CVE-2016-5696, CVE-2016-6130, CVE-2016-6327, CVE-2016-6480, CVE-2016-6828, CVE-2016-7042, CVE-2016-7097, CVE-2016-7425, CVE-2016-8658, CVE-2016-8666

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2912-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002422.html

SuSE SLES 12 SP1
noarch
kernel-source-3.12.67-60.64.18.1
kernel-devel-3.12.67-60.64.18.1
kernel-macros-3.12.67-60.64.18.1

x86_64
kernel-xen-base-debuginfo-3.12.67-60.64.18.1
kernel-xen-devel-3.12.67-60.64.18.1
kernel-default-base-3.12.67-60.64.18.1
kernel-xen-debuginfo-3.12.67-60.64.18.1
kernel-xen-base-3.12.67-60.64.18.1
kernel-default-debugsource-3.12.67-60.64.18.1
kernel-default-3.12.67-60.64.18.1
kernel-syms-3.12.67-60.64.18.1
kernel-default-debuginfo-3.12.67-60.64.18.1
kernel-default-base-debuginfo-3.12.67-60.64.18.1
kernel-xen-3.12.67-60.64.18.1
kernel-default-devel-3.12.67-60.64.18.1
kernel-xen-debugsource-3.12.67-60.64.18.1

SuSE SLED 12 SP1
x86_64
kernel-xen-devel-3.12.67-60.64.18.1
kernel-default-debugsource-3.12.67-60.64.18.1
kernel-default-extra-debuginfo-3.12.67-60.64.18.1
kernel-xen-debuginfo-3.12.67-60.64.18.1
kernel-default-devel-3.12.67-60.64.18.1
kernel-syms-3.12.67-60.64.18.1

kernel-default-3.12.67-60.64.18.1
kernel-xen-debugsource-3.12.67-60.64.18.1
kernel-default-debuginfo-3.12.67-60.64.18.1
kernel-default-extra-3.12.67-60.64.18.1
kernel-xen-3.12.67-60.64.18.1

noarch
kernel-source-3.12.67-60.64.18.1
kernel-devel-3.12.67-60.64.18.1
kernel-macros-3.12.67-60.64.18.1

145020 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2016:2893-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7032, CVE-2016-7076

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2893-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002414.html

SuSE SLED 12 SP2
x86_64
sudo-1.8.10p3-8.1
sudo-debugsource-1.8.10p3-8.1
sudo-debuginfo-1.8.10p3-8.1

SuSE SLES 12 SP2
x86_64
sudo-1.8.10p3-8.1
sudo-debugsource-1.8.10p3-8.1
sudo-debuginfo-1.8.10p3-8.1

145022 - SuSE SLES 11 SP4 SUSE-SU-2016:2891-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7032, CVE-2016-7076

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2891-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002413.html

SuSE SLES 11 SP4

i586
sudo-1.7.6p2-0.29.1

x86_64
sudo-1.7.6p2-0.29.1

145023 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2911-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2304, CVE-2016-5418, CVE-2016-5844, CVE-2016-6250, CVE-2016-8687, CVE-2016-8688, CVE-2016-8689

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2911-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002421.html

SuSE SLED 12 SP1
x86_64
libarchive13-debuginfo-3.1.2-25.1
libarchive-debugsource-3.1.2-25.1
libarchive13-3.1.2-25.1

SuSE SLES 12 SP2
x86_64
libarchive13-debuginfo-3.1.2-25.1
libarchive-debugsource-3.1.2-25.1
libarchive13-3.1.2-25.1

SuSE SLED 12 SP2
x86_64
libarchive13-debuginfo-3.1.2-25.1
libarchive-debugsource-3.1.2-25.1
libarchive13-3.1.2-25.1

SuSE SLES 12 SP1
x86_64
libarchive13-debuginfo-3.1.2-25.1
libarchive-debugsource-3.1.2-25.1
libarchive13-3.1.2-25.1

145024 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2896-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6321

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2896-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002417.html

SuSE SLED 12 SP1
x86_64
tar-debuginfo-1.27.1-11.1
tar-debugsource-1.27.1-11.1
tar-1.27.1-11.1

noarch
tar-lang-1.27.1-11.1

SuSE SLES 12 SP2
noarch
tar-lang-1.27.1-11.1

x86_64
tar-debuginfo-1.27.1-11.1
tar-debugsource-1.27.1-11.1
tar-1.27.1-11.1

SuSE SLED 12 SP2
x86_64
tar-debuginfo-1.27.1-11.1
tar-debugsource-1.27.1-11.1
tar-1.27.1-11.1

noarch
tar-lang-1.27.1-11.1

SuSE SLES 12 SP1
noarch
tar-lang-1.27.1-11.1

x86_64
tar-debuginfo-1.27.1-11.1
tar-debugsource-1.27.1-11.1
tar-1.27.1-11.1

145025 - SuSE SLES 11 SP4 SUSE-SU-2016:2895-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6321

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2895-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002416.html

SuSE SLES 11 SP4
i586
tar-1.26-1.2.10.1

x86_64
tar-1.26-1.2.10.1

145029 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:2904-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9680, CVE-2016-7032, CVE-2016-7076

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2904-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002420.html

SuSE SLES 12 SP1
x86_64
sudo-debuginfo-1.8.10p3-2.6.1
sudo-debugsource-1.8.10p3-2.6.1
sudo-1.8.10p3-2.6.1

SuSE SLED 12 SP1
x86_64
sudo-debuginfo-1.8.10p3-2.6.1
sudo-debugsource-1.8.10p3-2.6.1
sudo-1.8.10p3-2.6.1

160173 - CentOS 6 CESA-2016-2820 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8704, CVE-2016-8705

Description

The scan detected that the host is missing the following update:
CESA-2016-2820

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-November/022161.html

CentOS 6
x86_64
memcached-devel-1.4.4-3.el6_8.1
memcached-1.4.4-3.el6_8.1

i686
memcached-devel-1.4.4-3.el6_8.1
memcached-1.4.4-3.el6_8.1

160174 - CentOS 6 CESA-2016-2824 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0718

Description

The scan detected that the host is missing the following update:
CESA-2016-2824

Observation

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

http://lists.centos.org/pipermail/centos-announce/2016-November/022162.html

CentOS 6
x86_64
expat-2.0.1-13.el6_8
expat-devel-2.0.1-13.el6_8

i686
expat-2.0.1-13.el6_8
expat-devel-2.0.1-13.el6_8

163229 - Oracle Enterprise Linux ELSA-2016-2825 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5290

Description

The scan detected that the host is missing the following update:
ELSA-2016-2825

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-November/006541.html
http://oss.oracle.com/pipermail/el-errata/2016-November/006542.html

OEL7
x86_64
thunderbird-45.5.0-1.0.1.el7_3

OEL6
x86_64
thunderbird-45.5.0-1.0.1.el6_8

i386
thunderbird-45.5.0-1.0.1.el6_8

163230 - Oracle Enterprise Linux ELSA-2016-2820 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8704, CVE-2016-8705, CVE-2016-8706

Description

The scan detected that the host is missing the following update:
ELSA-2016-2820

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-November/006536.html

OEL6
x86_64
memcached-devel-1.4.4-3.el6_8.1
memcached-1.4.4-3.el6_8.1

i386
memcached-devel-1.4.4-3.el6_8.1
memcached-1.4.4-3.el6_8.1

163231 - Oracle Enterprise Linux ELSA-2016-2824 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-0718

Description

The scan detected that the host is missing the following update:
ELSA-2016-2824

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-November/006540.html
http://oss.oracle.com/pipermail/el-errata/2016-November/006539.html

OEL7
x86_64
expat-2.1.0-10.el7_3
expat-static-2.1.0-10.el7_3
expat-devel-2.1.0-10.el7_3

OEL6
x86_64
expat-2.0.1-13.el6_8
expat-devel-2.0.1-13.el6_8

i386
expat-2.0.1-13.el6_8

expat-devel-2.0.1-13.el6_8

175039 - Scientific Linux Security ERRATA Important: memcached on SL6.x i386/x86_64 (1611-4456)

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

Risk Level: High

CVE: CVE-2016-8704, CVE-2016-8705

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: memcached on SL6.x i386/x86_64 (1611-4456)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1611&L=scientific-linux-errata&F=&S=&P=4456

SL6
x86_64
memcached-1.4.4-3.el6_8.1
memcached-devel-1.4.4-3.el6_8.1
memcached-debuginfo-1.4.4-3.el6_8.1

i386
memcached-1.4.4-3.el6_8.1
memcached-devel-1.4.4-3.el6_8.1
memcached-debuginfo-1.4.4-3.el6_8.1

191400 - Fedora Linux 24 FEDORA-2016-49a72fb9bd Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7504, CVE-2016-7505, CVE-2016-7506, CVE-2016-9017, CVE-2016-9108, CVE-2016-9109, CVE-2016-9294

Description

The scan detected that the host is missing the following update:
FEDORA-2016-49a72fb9bd

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/2016/11/?count=200&page=2

Fedora Core 24

zathura-pdf-mupdf-0.3.0-3.fc24
mujs-0-6.20161031gita0ceaf5.fc24

191403 - Fedora Linux 24 FEDORA-2016-a0dc2c43d0 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7415

Description

The scan detected that the host is missing the following update:
FEDORA-2016-a0dc2c43d0

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/2016/11/?count=200&page=2

Fedora Core 24

icu-56.1-7.fc24

191407 - Fedora Linux 25 FEDORA-2016-4cf3e3f488 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7504, CVE-2016-7505, CVE-2016-7506, CVE-2016-9017, CVE-2016-9108, CVE-2016-9109, CVE-2016-9294

Description

The scan detected that the host is missing the following update:
FEDORA-2016-4cf3e3f488

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/2016/11/?count=200&page=3

Fedora Core 25

mujs-0-6.20161031gita0ceaf5.fc25
zathura-pdf-mupdf-0.3.0-3.fc25

191418 - Fedora Linux 23 FEDORA-2016-ee3a114958 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-8630, CVE-2016-8645, CVE-2016-9083, CVE-2016-9084

Description

The scan detected that the host is missing the following update:
FEDORA-2016-ee3a114958

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/2016/11/?count=200&page=3

Fedora Core 23

kernel-4.8.8-100.fc23

191420 - Fedora Linux 25 FEDORA-2016-db6ea7f449 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7415

Description

The scan detected that the host is missing the following update:
FEDORA-2016-db6ea7f449

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/2016/11/?count=200&page=3

Fedora Core 25

icu-57.1-4.fc25

20899 - (SYM16-020) Symantec Ghost Solution Suite DLL Loading Code Execution Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-6590

Description

An arbitrary code execution vulnerability exists in some versions of Symantec Ghost Solution Suite.

Observation

Symantec Ghost Solution Suite is a disk imaging software solution.

An arbitrary code execution vulnerability exists in some versions of Symantec Ghost Solution Suite. The flaw lies in how this software handles the loading of DLL dependencies. Successful exploitation of this vulnerability could allow a malicious user to execute arbitrary code. Exploitation of this vulnerability requires a non-privileged user to click on a malicious URL within a website or an email.

20900 - (VMSA-2016-0020) VMware vRealize Operations REST API Deserialization Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-7462

Description

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

Observation

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

A deserialization vulnerability is present in some versions of VMware vRealize Operations. The flaw lies in REST API. Successful exploitation could allow an attacker to write files with arbitrary content, move existing files into certain folders and cause a denial of service condition.

20906 - (VMSA-2016-0020) VMware vRealize Operations REST API Deserialization Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-7462

Description

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

Observation

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

A deserialization vulnerability is present in some versions of VMware vRealize Operations. The flaw lies in REST API. Successful exploitation could allow an attacker to write files with arbitrary content, move existing files into certain folders and cause a denial of service condition.

20918 - (SOL23946311) F5 BIG-IP Glibc Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-8776

Description

A vulnerability is present in glibc (GNU C Library) in some versions of F5 BIG-IP systems.

Observation

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

A vulnerability is present in glibc (GNU C Library) in some versions of F5 BIG-IP systems. The flaw lies in glibc component. Successful exploitation could allow a remote attacker to cause a denial of service condition or an information disclosure.

20931 - Apache Tomcat Multiple Vulnerabilities Prior To 8.0.39

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

Risk Level: Medium

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

Description

Multiple vulnerabilities are present in some versions of Apache Tomcat.

Observation

Apache Tomcat is a Java application server.

Multiple vulnerabilities are present in some versions of Apache Tomcat. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code, poison a web-cache, perform an XSS attack or obtain sensitive information.

145018 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2942-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1248

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2942-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002429.html

SuSE SLED 12 SP1
x86_64
vim-debugsource-7.4.326-7.1
vim-debuginfo-7.4.326-7.1
vim-7.4.326-7.1
gvim-7.4.326-7.1
gvim-debuginfo-7.4.326-7.1

noarch
vim-data-7.4.326-7.1

SuSE SLES 12 SP2
noarch
vim-data-7.4.326-7.1

x86_64
vim-debugsource-7.4.326-7.1
vim-debuginfo-7.4.326-7.1
vim-7.4.326-7.1
gvim-7.4.326-7.1
gvim-debuginfo-7.4.326-7.1

SuSE SLED 12 SP2
x86_64
vim-debugsource-7.4.326-7.1
vim-debuginfo-7.4.326-7.1
vim-7.4.326-7.1
gvim-7.4.326-7.1
gvim-debuginfo-7.4.326-7.1

noarch
vim-data-7.4.326-7.1

SuSE SLES 12 SP1
noarch
vim-data-7.4.326-7.1

x86_64
vim-debugsource-7.4.326-7.1
vim-debuginfo-7.4.326-7.1
vim-7.4.326-7.1
gvim-7.4.326-7.1
gvim-debuginfo-7.4.326-7.1

145021 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2016:2933-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3492, CVE-2016-5584, CVE-2016-5616, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6663, CVE-2016-7440, CVE-2016-8283

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2933-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002425.html

SuSE SLED 12 SP2
x86_64
mariadb-errormessages-10.0.28-17.2
libmysqlclient_r18-10.0.28-17.2
mariadb-10.0.28-17.2
libmysqlclient18-32bit-10.0.28-17.2
mariadb-client-debuginfo-10.0.28-17.2
mariadb-debuginfo-10.0.28-17.2
libmysqlclient_r18-32bit-10.0.28-17.2
mariadb-debugsource-10.0.28-17.2
mariadb-client-10.0.28-17.2
libmysqlclient18-10.0.28-17.2
libmysqlclient18-debuginfo-10.0.28-17.2
libmysqlclient18-debuginfo-32bit-10.0.28-17.2

SuSE SLES 12 SP2
x86_64
mariadb-errormessages-10.0.28-17.2
libmysqlclient18-debuginfo-32bit-10.0.28-17.2
mariadb-client-debuginfo-10.0.28-17.2
libmysqlclient18-32bit-10.0.28-17.2
mariadb-tools-10.0.28-17.2
mariadb-10.0.28-17.2
mariadb-debugsource-10.0.28-17.2
mariadb-client-10.0.28-17.2
libmysqlclient18-10.0.28-17.2
libmysqlclient18-debuginfo-10.0.28-17.2
mariadb-tools-debuginfo-10.0.28-17.2
mariadb-debuginfo-10.0.28-17.2

SuSE SLES 12 SP1
x86_64
mariadb-errormessages-10.0.28-17.2
libmysqlclient18-debuginfo-32bit-10.0.28-17.2
mariadb-client-debuginfo-10.0.28-17.2
libmysqlclient18-32bit-10.0.28-17.2
mariadb-tools-10.0.28-17.2
mariadb-10.0.28-17.2
mariadb-debugsource-10.0.28-17.2
mariadb-client-10.0.28-17.2
libmysqlclient18-10.0.28-17.2
libmysqlclient18-debuginfo-10.0.28-17.2
mariadb-tools-debuginfo-10.0.28-17.2
mariadb-debuginfo-10.0.28-17.2

SuSE SLED 12 SP1

x86_64
mariadb-errormessages-10.0.28-17.2
libmysqlclient_r18-10.0.28-17.2
mariadb-10.0.28-17.2
libmysqlclient18-32bit-10.0.28-17.2
mariadb-client-debuginfo-10.0.28-17.2
mariadb-debuginfo-10.0.28-17.2
libmysqlclient_r18-32bit-10.0.28-17.2
mariadb-debugsource-10.0.28-17.2
mariadb-client-10.0.28-17.2
libmysqlclient18-10.0.28-17.2
libmysqlclient18-debuginfo-10.0.28-17.2
libmysqlclient18-debuginfo-32bit-10.0.28-17.2

145028 - SuSE SLES 11 SP4 SUSE-SU-2016:2938-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1248

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2938-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002427.html

SuSE SLES 11 SP4
i586
vim-data-7.2-8.17.1
gvim-7.2-8.17.1
vim-base-7.2-8.17.1
vim-7.2-8.17.1

x86_64
vim-data-7.2-8.17.1
gvim-7.2-8.17.1
vim-base-7.2-8.17.1
vim-7.2-8.17.1

185494 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3139-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-1248

Description

The scan detected that the host is missing the following update:
USN-3139-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003641.html

Ubuntu 12.04

vim-gui-common_7.3.429-2ubuntu2.2
vim_7.3.429-2ubuntu2.2
vim-runtime_7.3.429-2ubuntu2.2
vim-common_7.3.429-2ubuntu2.2

Ubuntu 16.04

vim_7.4.1689-3ubuntu1.2
vim-gui-common_7.4.1689-3ubuntu1.2
vim-common_7.4.1689-3ubuntu1.2
vim-runtime_7.4.1689-3ubuntu1.2

Ubuntu 14.04

vim_7.4.052-1ubuntu3.1
vim-common_7.4.052-1ubuntu3.1
vim-runtime_7.4.052-1ubuntu3.1
vim-gui-common_7.4.052-1ubuntu3.1

Ubuntu 16.10

vim_7.4.1829-1ubuntu2.1
vim-common_7.4.1829-1ubuntu2.1
vim-runtime_7.4.1829-1ubuntu2.1
vim-gui-common_7.4.1829-1ubuntu2.1

191416 - Fedora Linux 23 FEDORA-2016-4f7d4df7b3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9186, CVE-2016-9187, CVE-2016-9188

Description

The scan detected that the host is missing the following update:
FEDORA-2016-4f7d4df7b3

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/2016/11/?count=200&page=3

Fedora Core 23

moodle-3.0.7-1.fc23

191419 - Fedora Linux 24 FEDORA-2016-026ee97af7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9186, CVE-2016-9187, CVE-2016-9188

Description

The scan detected that the host is missing the following update:
FEDORA-2016-026ee97af7

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/2016/11/?count=200&page=3

Fedora Core 24

moodle-3.1.3-1.fc24

20917 - (SOL40524634) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-0797

Description

A 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 vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the OpenSSL Component. Successful exploitation could allow an attacker to cause a denial of service condition or possibly have other unspecified impact in the target system.

20922 - (SOL06223540) F5 BIG-IP F5 TCP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-8240

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 Traffic Management Microkernel (TMM). Successful exploitation could allow an attacker to cause a denial-of-service condition.

20927 - (SOL21632201) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2011-5321

Description

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

Observation

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

A denial of service vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the Linux kernel. Successful exploitation could allow an attacker to cause a denial of service condition or possibly have other unspecified impact in the target system. This is a locally exploitable vulnerability.

182178 - FreeBSD Drupal Code Multiple Vulnerabilities (8db24888-b2f5-11e6-8153-00248c0c745d)

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

Risk Level: Medium

CVE: CVE-2016-9449, CVE-2016-9450, CVE-2016-9451, CVE-2016-9452

Description

The scan detected that the host is missing the following update:
Drupal Code -- Multiple Vulnerabilities (8db24888-b2f5-11e6-8153-00248c0c745d)

Observation

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

http://www.vuxml.org/freebsd/8db24888-b2f5-11e6-8153-00248c0c745d.html

Affected packages:
7.0 <= drupal7 < 7.52
8.0.0 <= drupal8 < 8.2.3

182180 - FreeBSD libwww Multiple Vulnerabilities (18449f92-ab39-11e6-8011-005056925db4)

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

Risk Level: Medium

CVE: CVE-2005-3183, CVE-2009-3560, CVE-2009-3720

Description

The scan detected that the host is missing the following update:
libwww -- multiple vulnerabilities (18449f92-ab39-11e6-8011-005056925db4)

Observation

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

http://www.vuxml.org/freebsd/18449f92-ab39-11e6-8011-005056925db4.html

Affected packages:
libwww < 5.4.0_6

191401 - Fedora Linux 23 FEDORA-2016-8e39076950 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6170, CVE-2016-8864

Description

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

FEDORA-2016-8e39076950

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/2016/11/?count=200&page=3

Fedora Core 23

bind99-9.9.9-4.P4.fc23

191405 - Fedora Linux 23 FEDORA-2016-605fd98c32 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-8864

Description

The scan detected that the host is missing the following update:
FEDORA-2016-605fd98c32

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/2016/11/?count=200&page=2

Fedora Core 23

bind-9.10.4-2.P4.fc23

191409 - Fedora Linux 25 FEDORA-2016-95b1be8a3d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9449, CVE-2016-9450, CVE-2016-9451, CVE-2016-9452

Description

The scan detected that the host is missing the following update:
FEDORA-2016-95b1be8a3d

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/2016/11/?count=200&page=1

Fedora Core 25

drupal7-7.52-1.fc25

191410 - Fedora Linux 23 FEDORA-2016-ff9a74c6dc Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9449, CVE-2016-9450, CVE-2016-9451, CVE-2016-9452

Description

The scan detected that the host is missing the following update:
FEDORA-2016-ff9a74c6dc

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/2016/11/?count=200&page=1

Fedora Core 23

drupal7-7.52-1.fc23

191414 - Fedora Linux 25 FEDORA-2016-1637001349 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9296

Description

The scan detected that the host is missing the following update:
FEDORA-2016-1637001349

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/2016/11/?count=200&page=1

Fedora Core 25

p7zip-16.02-2.fc25

191415 - Fedora Linux 24 FEDORA-2016-1cc5edde49 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9449, CVE-2016-9450, CVE-2016-9451, CVE-2016-9452

Description

The scan detected that the host is missing the following update:
FEDORA-2016-1cc5edde49

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/2016/11/?count=200&page=1

Fedora Core 24

drupal7-7.52-1.fc24

20908 - IBM Tivoli Storage Manager for Virtual Environments Authentication Bypass Vulnerability (swg21988781)

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

Risk Level: Medium

CVE: CVE-2016-2988

Description

An authentication bypass vulnerability is present in some versions of IBM Tivoli Storage Manager for Virtual Environments.

Observation

IBM Tivoli Storage Manager for Virtual Environments is a software solution for administrative tasks of storage instances in virtualization environments.

An authentication bypass vulnerability is present in some versions of IBM Tivoli Storage Manager for Virtual Environments. The flaw lies in the component known as Data Protection for VMware GUI. Successful exploitation could allow a malicious user without elevated privileges to execute tasks that require Tivoli Storage Manager administrative permissions, such as: backup scheduling and configuration tasks.

20923 - (VMSA-2016-0022) VMware vSphere Client XML External Entity Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-7458

Description

An information disclosure vulnerability is present in some versions of VMware vSphere Client.

Observation

VMware vSphere Client is a software that allows the management of VMware infrastructure.

An information disclosure vulnerability is present in some versions of VMware vSphere Client. The flaw lies in XML parsing. Successful exploitation from a remote attacker could allow access to potentially sensitive information.

163232 - Oracle Enterprise Linux ELSA-2016-2819 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-7239, CVE-2016-8704, CVE-2016-8705, CVE-2016-8706

Description

The scan detected that the host is missing the following update:
ELSA-2016-2819

Observation

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

http://oss.oracle.com/pipermail/el-errata/2016-November/006535.html

OEL7
x86_64
memcached-devel-1.4.15-10.el7_3.1
memcached-1.4.15-10.el7_3.1

185491 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3137-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-7146, CVE-2016-7148, CVE-2016-9119

Description

The scan detected that the host is missing the following update:
USN-3137-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003638.html

Ubuntu 12.04

python-moinmoin_1.9.3-1ubuntu2.3

Ubuntu 16.04

python-moinmoin_1.9.8-1ubuntu1.16.04.1

Ubuntu 14.04

python-moinmoin_1.9.7-1ubuntu2.1

Ubuntu 16.10

python-moinmoin_1.9.8-1ubuntu1.16.10.1

130637 - Debian Linux 8.0 DSA-3724-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636

Description

The scan detected that the host is missing the following update:
DSA-3724-1

Observation

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

http://www.debian.org/security/2016/dsa-3724

Debian 8.0
all
gstreamer0.10-plugins-good-dbg_0.10.31-3+nmu4+deb8u2

gstreamer0.10-pulseaudio_0.10.31-3+nmu4+deb8u2
gstreamer0.10-gconf_0.10.31-3+nmu4+deb8u2
gstreamer0.10-plugins-good_0.10.31-3+nmu4+deb8u2
gstreamer0.10-plugins-good-doc_0.10.31-3+nmu4+deb8u2

130638 - Debian Linux 8.0 DSA-3723-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9634, CVE-2016-9635, CVE-2016-9636

Description

The scan detected that the host is missing the following update:
DSA-3723-1

Observation

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

http://www.debian.org/security/2016/dsa-3723

Debian 8.0
all
gstreamer1.0-pulseaudio_1.4.4-2+deb8u2
gstreamer1.0-plugins-good-dbg_1.4.4-2+deb8u2
gstreamer1.0-plugins-good_1.4.4-2+deb8u2
gstreamer1.0-plugins-good-doc_1.4.4-2+deb8u2

130639 - Debian Linux 8.0 DSA-3726-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7799, CVE-2016-7906, CVE-2016-8677, CVE-2016-8862, CVE-2016-9556, CVE-2016-9559

Description

The scan detected that the host is missing the following update:
DSA-3726-1

Observation

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

http://www.debian.org/security/2016/dsa-3726

Debian 8.0
all
imagemagick_8:6.8.9.9-5+deb8u6

145016 - SuSE Linux 13.2 openSUSE-SU-2016:2888-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-8972

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2016:2888-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2016-11/msg00105.html

SuSE Linux 13.2
x86_64
gnuchess-debugsource-6.0.2-6.3.1
gnuchess-debuginfo-6.0.2-6.3.1
gnuchess-6.0.2-6.3.1

i586
gnuchess-debugsource-6.0.2-6.3.1
gnuchess-debuginfo-6.0.2-6.3.1
gnuchess-6.0.2-6.3.1

145026 - SuSE SLES 12 SP1, 12 SP2 SUSE-SU-2016:2915-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-4983

Description

The scan detected that the host is missing the following update:
SUSE-SU-2016:2915-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2016-November/002423.html

SuSE SLES 12 SP1
x86_64
dovecot22-debuginfo-2.2.13-4.1
dovecot22-2.2.13-4.1
dovecot22-debugsource-2.2.13-4.1
dovecot22-backend-mysql-2.2.13-4.1
dovecot22-backend-pgsql-debuginfo-2.2.13-4.1
dovecot22-backend-sqlite-debuginfo-2.2.13-4.1
dovecot22-backend-mysql-debuginfo-2.2.13-4.1
dovecot22-backend-sqlite-2.2.13-4.1
dovecot22-backend-pgsql-2.2.13-4.1

SuSE SLES 12 SP2
x86_64
dovecot22-debuginfo-2.2.13-4.1
dovecot22-2.2.13-4.1
dovecot22-debugsource-2.2.13-4.1
dovecot22-backend-mysql-2.2.13-4.1
dovecot22-backend-pgsql-debuginfo-2.2.13-4.1
dovecot22-backend-sqlite-debuginfo-2.2.13-4.1

dovecot22-backend-mysql-debuginfo-2.2.13-4.1
dovecot22-backend-sqlite-2.2.13-4.1
dovecot22-backend-pgsql-2.2.13-4.1

182179 - FreeBSD Remote-Code-Execution Vulnerability In Mysql And Its Variants CVE 2016-6662 (dc596a17-7a9e-11e6-b034-f0def167eeea)

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:
Remote-Code-Execution vulnerability in mysql and its variants CVE 2016-6662 (dc596a17-7a9e-11e6-b034-f0def167eeea)

Observation

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

http://www.vuxml.org/freebsd/dc596a17-7a9e-11e6-b034-f0def167eeea.html

Affected packages:
mysql57-client < 5.7.15
mysql57-server < 5.7.15
mysql56-client < 5.6.33
mysql56-server < 5.6.33
mysql55-client < 5.5.52
mysql55-server < 5.5.52

182181 - FreeBSD phpMyAdmin Multiple Vulnerabilities (6fe72178-b2e3-11e6-8b2a-6805ca0b3d42)

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

Risk Level: Low

CVE: CVE-2016-4412, CVE-2016-6632, CVE-2016-6633

Description

The scan detected that the host is missing the following update:
phpMyAdmin -- multiple vulnerabilities (6fe72178-b2e3-11e6-8b2a-6805ca0b3d42)

Observation

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

http://www.vuxml.org/freebsd/6fe72178-b2e3-11e6-8b2a-6805ca0b3d42.html

Affected packages:
4.6.0 <= phpMyAdmin < 4.6.5

182182 - FreeBSD mozilla Data: URL Can Inherit Wrong Origin After An HTTP Redirect (f90fce70-ecfa-4f4d-9ee8-c476dbf4bf0e)

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

Risk Level: Low

CVE: CVE-2016-9078

Description

The scan detected that the host is missing the following update:
mozilla -- data: URL can inherit wrong origin after an HTTP redirect (f90fce70-ecfa-4f4d-9ee8-c476dbf4bf0e)

Observation

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

http://www.vuxml.org/freebsd/f90fce70-ecfa-4f4d-9ee8-c476dbf4bf0e.html

Affected packages:
firefox < 50.0.1,1

182183 - FreeBSD Roundcube Arbitrary Command Execution (125f5958-b611-11e6-a9a5-b499baebfeaf)

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:
Roundcube -- arbitrary command execution (125f5958-b611-11e6-a9a5-b499baebfeaf)

Observation

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

http://www.vuxml.org/freebsd/125f5958-b611-11e6-a9a5-b499baebfeaf.html

Affected packages:
roundcube < 1.2.3,1

182184 - FreeBSD subversion Unrestricted XML Entity Expansion In Mod_dontdothat And Subversionclients Using Http (s) (ac256985-b6a9-11e6-

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

Risk Level: Low

CVE: CVE-2016-8734

Description

The scan detected that the host is missing the following update:
subversion -- Unrestricted XML entity expansion in mod_dontdothat and Subversionclients using http(s) (ac256985-b6a9-11e6-a3bf-206a8a720317)

Observation

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

http://www.vuxml.org/freebsd/ac256985-b6a9-11e6-a3bf-206a8a720317.html

Affected packages:
subversion18 < 1.8.17
subversion < 1.9.5

185490 - Ubuntu Linux 16.04, 16.10 USN-3138-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9243

Description

The scan detected that the host is missing the following update:
USN-3138-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003640.html

Ubuntu 16.10

python-cryptography_1.5-2ubuntu0.1
python3-cryptography_1.5-2ubuntu0.1

Ubuntu 16.04

python3-cryptography_1.2.3-1ubuntu0.1
python-cryptography_1.2.3-1ubuntu0.1

185492 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3136-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-8649

Description

The scan detected that the host is missing the following update:
USN-3136-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003637.html

Ubuntu 16.04

liblxc1_2.0.5-0ubuntu1~ubuntu16.04.3
lxc1_2.0.5-0ubuntu1~ubuntu16.04.3

Ubuntu 14.04

lxc_1.0.8-0ubuntu0.4
liblxc1_1.0.8-0ubuntu0.4

Ubuntu 16.10

lxc1_2.0.5-0ubuntu1.2
liblxc1_2.0.5-0ubuntu1.2

185493 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3135-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
USN-3135-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2016-November/003639.html

Ubuntu 12.04

gstreamer0.10-plugins-good_0.10.31-1ubuntu1.4

Ubuntu 16.04

gstreamer1.0-plugins-good_1.8.2-1ubuntu0.3

Ubuntu 14.04

gstreamer0.10-plugins-good_0.10.31-3+nmu1ubuntu5.2
gstreamer1.0-plugins-good_1.2.4-1~ubuntu1.3

Ubuntu 16.10

gstreamer1.0-plugins-good_1.8.3-1ubuntu1.2

191399 - Fedora Linux 25 FEDORA-2016-df20b90635 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9400

Description

The scan detected that the host is missing the following update:
FEDORA-2016-df20b90635

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/2016/11/?count=200&page=1

Fedora Core 25

teeworlds-0.6.4-2.fc25

191402 - Fedora Linux 23 FEDORA-2016-48614c8b69 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7076

Description

The scan detected that the host is missing the following update:
FEDORA-2016-48614c8b69

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/2016/11/?count=200&page=2

Fedora Core 23

sudo-1.8.18p1-1.fc23

191404 - Fedora Linux 25 FEDORA-2016-5a625412c2 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-2016-5a625412c2

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/2016/11/?count=200&page=1

Fedora Core 25

vagrant-1.8.5-2.fc25

191406 - Fedora Linux 23 FEDORA-2016-7470a63cd1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9400

Description

The scan detected that the host is missing the following update:
FEDORA-2016-7470a63cd1

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/2016/11/?count=200&page=1

Fedora Core 23

teeworlds-0.6.4-1.fc23

191408 - Fedora Linux 24 FEDORA-2016-24ffcb9a47 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-2016-24ffcb9a47

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/2016/11/?count=200&page=1

Fedora Core 24

vagrant-1.8.1-5.fc24

191411 - Fedora Linux 24 FEDORA-2016-16a522f9a6 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9400

Description

The scan detected that the host is missing the following update:
FEDORA-2016-16a522f9a6

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/2016/11/?count=200&page=1

Fedora Core 24

teeworlds-0.6.4-2.fc24

191412 - Fedora Linux 23 FEDORA-2016-15d4c05a19 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7977, CVE-2016-8602

Description

The scan detected that the host is missing the following update:
FEDORA-2016-15d4c05a19

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/2016/11/?count=200&page=3

Fedora Core 23

ghostscript-9.20-5.fc23

191413 - Fedora Linux 23 FEDORA-2016-7b335750d8 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-2016-7b335750d8

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/2016/11/?count=200&page=1

Fedora Core 23

vagrant-1.8.1-3.fc23

191417 - Fedora Linux 25 FEDORA-2016-24478a88fe 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-2016-24478a88fe

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/2016/11/?count=200&page=2

Fedora Core 25

python-tornado-4.4.2-1.fc25

191421 - Fedora Linux 24 FEDORA-2016-54fd3bf412 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-1249

Description

The scan detected that the host is missing the following update:
FEDORA-2016-54fd3bf412

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/2016/11/?count=200&page=2

Fedora Core 24

perl-DBD-MySQL-4.039-1.fc24

ENHANCED CHECKS

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

181963 - FreeBSD NSS Multiple Vulnerabilities (32166082-53fa-41fa-b081-207e7a989a0a)

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

Risk Level: High

CVE: CVE-2016-2834

Update Details

FASLScript is updated

19879 - (SOL81903701) F5 BIG-IP Libpng Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-8472

Update Details

Recommendation is updated

19881 - (SOL95698826) F5 BIG-IP LZO Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-4607

Update Details

Recommendation is updated

19883 - (SOL63519101) F5 BIG-IP QEMU Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-8106, CVE-2015-3209, CVE-2015-5165, CVE-2015-5279, CVE-2015-7504, CVE-2015-7512

Update Details

Recommendation is updated

19827 - (SOL62012529) F5 BIG-IP BIND Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-1286

Update Details

Recommendation is updated Documentation is updated

20732 - Novell Sentinel Vulnerability Prior To 7.4.3.0

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1000031

Update Details

FASLScript is updated

20889 - IBM AIX Bind Multiple Vulnerabilities (bind_advisory13)

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

Risk Level: High

CVE: CVE-2016-2775, CVE-2016-2776

Update Details

Risk is updated

20890 - IBM AIX OpenSSL Multiple Vulnerabilities (openssl_advisory21)

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

Risk Level: High

CVE: CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6306, CVE-2016-7052

Update Details

Risk is updated

130616 - Debian Linux 8.0 DSA-3701-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1247

Update Details

Risk is updated

184856 - Ubuntu Linux 12.04 USN-2640-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-1328

Update Details
Risk is updated

184859 - Ubuntu Linux 15.04 USN-2647-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-1328

Update Details
Risk is updated

184861 - Ubuntu Linux 14.04 USN-2643-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-1328

Update Details
Risk is updated

184862 - Ubuntu Linux 12.04 USN-2642-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-1328

Update Details
Risk is updated

184865 - Ubuntu Linux 14.10 USN-2646-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-1328

Update Details
Risk is updated

184869 - Ubuntu Linux 12.04 USN-2641-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-1328

Update Details

Risk is updated

184870 - Ubuntu Linux 14.04 USN-2644-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-1328

Update Details
Risk is updated

184874 - Ubuntu Linux 14.04 USN-2645-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-1328

Update Details
Risk is updated

184875 - Ubuntu Linux 14.10 USN-2646-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-1328

Update Details
Risk is updated

184877 - Ubuntu Linux 12.04 USN-2640-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-1328

Update Details
Risk is updated

184880 - Ubuntu Linux 14.04 USN-2644-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2015-1328

Update Details
Risk is updated

184881 - Ubuntu Linux 12.04 USN-2642-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High

CVE: CVE-2015-1328

Update Details

Risk is updated

184882 - Ubuntu Linux 14.04 USN-2643-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1328

Update Details

Risk is updated

184884 - Ubuntu Linux 12.04 USN-2641-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1328

Update Details

Risk is updated

185456 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3114-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1247

Update Details

Risk is updated

191332 - Fedora Linux 24 FEDORA-2016-96d276367e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9083, CVE-2016-9084

Update Details

Risk is updated

19877 - (SOL98102572) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7990

Update Details

Recommendation is updated

130631 - Debian Linux 8.0 DSA-3722-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-1248

Update Details
Risk is updated

16885 - (SOL15278) F5 BIG-IP SSL Renegotiation Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5
Risk Level: Medium
CVE: CVE-2011-1473

Update Details
Recommendation is updated Documentation is updated FASLScript is updated

20584 - (SOL62655427) F5 BIG-IP Libjpeg-turbo Vulnerability

Category: SSH Module -> NonIntrusive -> F5
Risk Level: Medium
CVE: CVE-2013-6630

Update Details
Recommendation is updated

20901 - (SA-CORE-2016-005) Drupal Core Multiple Vulnerabilities

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server
Risk Level: Medium
CVE: CVE-2016-9449, CVE-2016-9450, CVE-2016-9451, CVE-2016-9452

Update Details
Risk is updated

130635 - Debian Linux 8.0 DSA-3718-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-9449, CVE-2016-9451

Update Details
Risk is updated

191377 - Fedora Linux 25 FEDORA-2016-876deae183 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-8630

Update Details

Risk is updated

191387 - Fedora Linux 24 FEDORA-2016-14c4187e3a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-8630

Update Details
Risk is updated

191389 - Fedora Linux 24 FEDORA-2016-3548475bca Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-8645

Update Details
Risk is updated

191394 - Fedora Linux 25 FEDORA-2016-29cde72f15 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-8645

Update Details
Risk is updated

182177 - FreeBSD moodle Multiple Vulnerabilities (f6565fbf-ab9e-11e6-ae1b-002590263bf5)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2016-8642, CVE-2016-8643, CVE-2016-8644

Update Details
CVE is updated

191368 - Fedora Linux 25 FEDORA-2016-8f9d466bcc Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2016-5416

Update Details
CVE 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

70109 - symantec.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.