

MCAFFEE 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

22760 - Splunk Enterprise Multiple SAML Vulnerabilities (SP-CAAAP3K)

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

Multiple vulnerabilities are present in some versions of Splunk Enterprise.

Observation

Splunk Enterprise is a platform for real-time operational intelligence.

Multiple vulnerabilities are present in some versions of Splunk Enterprise. The flaws lie in all components running Splunk Web with SAML authentication enabled. Successful exploitation could allow an attacker to impersonate another user account.

22778 - (HPESBHF03768) HPE Intelligent Management Center Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-12487, CVE-2017-12488, CVE-2017-12489, CVE-2017-12490, CVE-2017-12491, CVE-2017-12492, CVE-2017-12493, CVE-2017-12494, CVE-2017-12495, CVE-2017-12496, CVE-2017-12497, CVE-2017-12498, CVE-2017-12499, CVE-2017-12500, CVE-2017-12501, CVE-2017-12502, CVE-2017-12503, CVE-2017-12504, CVE-2017-12505, CVE-2017-12506, CVE-2017-12507, CVE-2017-12508, CVE-2017-12509, CVE-2017-12510, CVE-2017-12511, CVE-2017-12512, CVE-2017-12513, CVE-2017-12514, CVE-2017-12515, CVE-2017-12516, CVE-2017-12517, CVE-2017-12518, CVE-2017-12519, CVE-2017-12520, CVE-2017-12521, CVE-2017-12522, CVE-2017-12523, CVE-2017-12524, CVE-2017-12525, CVE-2017-12526, CVE-2017-12527, CVE-2017-12528, CVE-2017-12529, CVE-2017-12530, CVE-2017-12531, CVE-2017-12532, CVE-2017-12533, CVE-2017-12534, CVE-2017-12535, CVE-2017-12536, CVE-2017-12537, CVE-2017-12538, CVE-2017-12539, CVE-2017-12540, CVE-2017-12541

Description

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

Observation

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

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

22787 - (HPESBHF03745) HPE Intelligent Management Center Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-5816, CVE-2017-5817, CVE-2017-5818, CVE-2017-5819, CVE-2017-8956

Description

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

Observation

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

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

22774 - (APSB17-37) Vulnerability In Adobe DNG Converter

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

Risk Level: High

CVE: CVE-2017-11295

Description

A memory corruption vulnerability is present in some versions of Adobe DNG Converter.

Observation

Adobe DNG Converter is a software used to convert image to DNG format.

A memory corruption vulnerability is present in some versions of Adobe DNG Converter. The flaw lies in unspecified component. Successful exploitation could allow an attacker to execute arbitrary code.

The update provided by Adobe bulletin APSB17-37 resolves this issue. The target system appears to be missing this update.

96047 - Fedora Linux 25 FEDORA-2017-d008ecf87a Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16641, CVE-2017-16660, CVE-2017-16661, CVE-2017-16785

Description

The scan detected that the host is missing the following update:
FEDORA-2017-d008ecf87a

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/2017/11/?count=200&page=1>

Fedora Core 25

cacti-1.1.28-1.fc25

96052 - Fedora Linux 26 FEDORA-2017-9762a831b2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16641, CVE-2017-16660, CVE-2017-16661, CVE-2017-16785

Description

The scan detected that the host is missing the following update:
FEDORA-2017-9762a831b2

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/2017/11/?count=200&page=2>

Fedora Core 26

cacti-1.1.28-1.fc26

146105 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3051-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16641, CVE-2017-16660, CVE-2017-16661, CVE-2017-16785

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3051-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00063.html>

SuSE Linux 42.2

i586

cacti-spine-debugsource-1.1.28-7.13.1

cacti-spine-1.1.28-7.13.1

cacti-spine-debuginfo-1.1.28-7.13.1

noarch

cacti-doc-1.1.28-16.13.1

cacti-1.1.28-16.13.1

x86_64

cacti-spine-debugsource-1.1.28-7.13.1

cacti-spine-1.1.28-7.13.1

cacti-spine-debuginfo-1.1.28-7.13.1

SuSE Linux 42.3

i586

cacti-spine-debugsource-1.1.28-20.1

cacti-spine-1.1.28-20.1

cacti-spine-debuginfo-1.1.28-20.1

noarch

cacti-1.1.28-29.1

cacti-doc-1.1.28-29.1

x86_64
cacti-spine-debugsource-1.1.28-20.1
cacti-spine-1.1.28-20.1
cacti-spine-debuginfo-1.1.28-20.1

192989 - Fedora Linux 27 FEDORA-2017-cf75844225 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16641, CVE-2017-16660, CVE-2017-16661, CVE-2017-16785

Description

The scan detected that the host is missing the following update:
FEDORA-2017-cf75844225

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/2017/11/?count=200&page=2>

Fedora Core 27

cacti-1.1.28-1.fc27

22781 - (VMSA-2017-0018) VMware Fusion Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-4934, CVE-2017-4938

Description

Multiple vulnerabilities are present in some versions of VMware Fusion.

Observation

VMware Fusion is a popular virtualization platform.

Multiple vulnerabilities are present in some versions of VMware Fusion. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary remote code or to cause a denial-of-service.

22786 - (HPESBHF03719) HPE Intelligent Management Center Information Disclosure Vulnerability

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

Risk Level: High

CVE: CVE-2017-5797

Description

An information disclosure vulnerability is present in some versions of HPE Intelligent Management Center.

Observation

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

An information disclosure vulnerability is present in some versions of HPE Intelligent Management Center. The flaw lies in the iMC Service Operation Module (SOM). Successful exploitation could allow an attacker to obtain sensitive information.

22761 - (VMSA-2017-0018) VMware Horizon View Client Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-4935, CVE-2017-4936, CVE-2017-4937

Description

Multiple vulnerabilities are present in some versions of VMware Horizon View Client.

Observation

VMware Horizon View Client is VMWare desktop-virtualization product.

Multiple vulnerabilities are present in some versions of VMware Horizon View Client. The flaws are due to multiple out-of-bounds read in JPEG2000 parser. Successful exploitation could allow an attacker to execute arbitrary code or cause a denial of service condition on the Windows OS running VMware Horizon View Client.

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

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

Risk Level: High

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

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 lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information.

22767 - (VMSA-2017-0018) VMware Workstation Player Multiple Vulnerabilities I

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

Risk Level: High

CVE: CVE-2017-4934, CVE-2017-4938

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 cause denial of services or execute arbitrary code.

22768 - (VMSA-2017-0018) VMware Workstation Player Multiple Vulnerabilities I

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-4934, CVE-2017-4938

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 cause denial of services or execute arbitrary code.

22771 - (K01837042) F5 BIG-IP Multiple Wireshark Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-8711, CVE-2015-8714, CVE-2015-8716, CVE-2015-8717, CVE-2015-8718, CVE-2015-8720, CVE-2015-8721, CVE-2015-8723, CVE-2015-8725, CVE-2015-8729, CVE-2015-8730, CVE-2015-8733, CVE-2016-2523, CVE-2016-4006, CVE-2016-4078, CVE-2016-4079, CVE-2016-4080, CVE-2016-4081, CVE-2016-4085

Description

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

22773 - AutomationDirect GS Drives Configuration Software DLL Hijacking Vulnerability

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

Risk Level: High

CVE: CVE-2017-14020

Description

A DLL hijacking vulnerability is present in some versions of AutomationDirect GS Drives Configuration Software.

Observation

AutomationDirect GS Drives Configuration Software is a HMI/SCADA software used to create robust HMI screens to control machine, process.

A DLL hijacking vulnerability is present in some versions of AutomationDirect GS Drives Configuration Software. The flaw is related to an uncontrolled search path element. Successful exploitation could allow an attacker to execute arbitrary code on the system.

22775 - (VMSA-2017-0018) VMware Workstation Player Multiple Vulnerabilities II

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

Risk Level: High

CVE: CVE-2017-4935, CVE-2017-4936, CVE-2017-4937, CVE-2017-4939

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 cause denial of services or execute arbitrary code.

22776 - (VMSA-2017-0018) VMware Workstation Pro Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-4934, CVE-2017-4935, CVE-2017-4936, CVE-2017-4937, CVE-2017-4938, CVE-2017-4939

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 execute arbitrary code and cause denial of service.

22779 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To ESR 52.5

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

Risk Level: High

CVE: CVE-2017-7826, CVE-2017-7828, CVE-2017-7830

Description

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

Observation

Mozilla Firefox ESR is a popular web browser.

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

22780 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To ESR 52.5

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-7826, CVE-2017-7828, CVE-2017-7830

Description

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

Observation

Mozilla Firefox ESR is a popular web browser.

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

22782 - (K54924436) F5 BIG-IP PHP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-8865

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 PHP. Successful exploitation could allow an attacker to cause a denial of service condition.

96043 - Fedora Linux 26 FEDORA-2017-2500a024ef Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15592, CVE-2017-15595

Description

The scan detected that the host is missing the following update:
FEDORA-2017-2500a024ef

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/2017/11/?count=200&page=1>

Fedora Core 26

xen-4.8.2-7.fc26

96045 - Fedora Linux 26 FEDORA-2017-0929e71b41 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12629

Description

The scan detected that the host is missing the following update:
FEDORA-2017-0929e71b41

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/2017/11/?count=200&page=1>

Fedora Core 26

lucene4-4.10.4-11.fc26

141779 - Red Hat Enterprise Linux RHSA-2017-3269 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16844

Description

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

RHSA-2017-3269

Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2017-November/msg00037.html>

RHEL7D

x86_64

procmail-3.22-36.el7_4.1

procmail-debuginfo-3.22-36.el7_4.1

RHEL7S

x86_64

procmail-3.22-36.el7_4.1

procmail-debuginfo-3.22-36.el7_4.1

RHEL7WS

x86_64

procmail-3.22-36.el7_4.1

procmail-debuginfo-3.22-36.el7_4.1

141782 - Red Hat Enterprise Linux RHSA-2017-3260 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14746, CVE-2017-15275

Description

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

RHSA-2017-3260

Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2017-November/msg00030.html>

RHEL7D

x86_64

libwbclient-devel-4.6.2-12.el7_4
samba-devel-4.6.2-12.el7_4
libsmbclient-4.6.2-12.el7_4
samba-4.6.2-12.el7_4
libsmbclient-devel-4.6.2-12.el7_4
samba-libs-4.6.2-12.el7_4
samba-winbind-krb5-locator-4.6.2-12.el7_4
samba-dc-4.6.2-12.el7_4
samba-debuginfo-4.6.2-12.el7_4
samba-krb5-printing-4.6.2-12.el7_4
samba-winbind-modules-4.6.2-12.el7_4
samba-test-4.6.2-12.el7_4
samba-vfs-glusterfs-4.6.2-12.el7_4
samba-winbind-clients-4.6.2-12.el7_4
libwbclient-4.6.2-12.el7_4
samba-common-tools-4.6.2-12.el7_4
samba-dc-libs-4.6.2-12.el7_4
samba-python-4.6.2-12.el7_4
samba-common-libs-4.6.2-12.el7_4
samba-client-libs-4.6.2-12.el7_4
samba-test-libs-4.6.2-12.el7_4
samba-winbind-4.6.2-12.el7_4
samba-client-4.6.2-12.el7_4

noarch

samba-pidl-4.6.2-12.el7_4
samba-common-4.6.2-12.el7_4

RHEL7S

noarch

samba-pidl-4.6.2-12.el7_4
samba-common-4.6.2-12.el7_4

x86_64

libwbclient-devel-4.6.2-12.el7_4
samba-winbind-clients-4.6.2-12.el7_4
samba-krb5-printing-4.6.2-12.el7_4
samba-devel-4.6.2-12.el7_4
libsmbclient-4.6.2-12.el7_4
samba-dc-4.6.2-12.el7_4
libsmbclient-devel-4.6.2-12.el7_4
samba-4.6.2-12.el7_4
samba-winbind-krb5-locator-4.6.2-12.el7_4
samba-libs-4.6.2-12.el7_4
samba-python-4.6.2-12.el7_4
samba-test-4.6.2-12.el7_4
samba-vfs-glusterfs-4.6.2-12.el7_4
samba-debuginfo-4.6.2-12.el7_4
libwbclient-4.6.2-12.el7_4
samba-common-tools-4.6.2-12.el7_4
samba-dc-libs-4.6.2-12.el7_4
samba-winbind-modules-4.6.2-12.el7_4
samba-common-libs-4.6.2-12.el7_4
samba-client-libs-4.6.2-12.el7_4
samba-test-libs-4.6.2-12.el7_4
samba-winbind-4.6.2-12.el7_4
samba-client-4.6.2-12.el7_4

RHEL7WS

x86_64

libwbclient-devel-4.6.2-12.el7_4

samba-winbind-clients-4.6.2-12.el7_4

samba-krb5-printing-4.6.2-12.el7_4

samba-devel-4.6.2-12.el7_4

libsmbclient-4.6.2-12.el7_4

samba-dc-4.6.2-12.el7_4

libsmbclient-devel-4.6.2-12.el7_4

samba-4.6.2-12.el7_4

samba-winbind-krb5-locator-4.6.2-12.el7_4

samba-libs-4.6.2-12.el7_4

samba-python-4.6.2-12.el7_4

samba-test-4.6.2-12.el7_4

samba-vfs-glusterfs-4.6.2-12.el7_4

samba-debuginfo-4.6.2-12.el7_4

libwbclient-4.6.2-12.el7_4

samba-common-tools-4.6.2-12.el7_4

samba-dc-libs-4.6.2-12.el7_4

samba-winbind-modules-4.6.2-12.el7_4

samba-common-libs-4.6.2-12.el7_4

samba-client-libs-4.6.2-12.el7_4

samba-test-libs-4.6.2-12.el7_4

samba-winbind-4.6.2-12.el7_4

samba-client-4.6.2-12.el7_4

noarch

samba-pidl-4.6.2-12.el7_4

samba-common-4.6.2-12.el7_4

146085 - SuSE SLED 12 SP2, 12 SP3 SUSE-SU-2017:3062-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

SUSE-SU-2017:3062-1

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-November/003407.html>

SuSE SLED 12 SP3

x86_64

gimp-debuginfo-2.8.18-9.3.26

gimp-plugins-python-2.8.18-9.3.26

gimp-2.8.18-9.3.26

libgimpui-2_0-0-debuginfo-2.8.18-9.3.26

libgimp-2_0-0-debuginfo-2.8.18-9.3.26

libgimp-2_0-0-2.8.18-9.3.26

libgimpui-2_0-0-2.8.18-9.3.26

gimp-plugins-python-debuginfo-2.8.18-9.3.26

gimp-debugsource-2.8.18-9.3.26

noarch
gimp-lang-2.8.18-9.3.26

SuSE SLED 12 SP2
x86_64
gimp-debuginfo-2.8.18-9.3.26
gimp-plugins-python-2.8.18-9.3.26
gimp-2.8.18-9.3.26
libgimpui-2_0-0-debuginfo-2.8.18-9.3.26
libgimp-2_0-0-debuginfo-2.8.18-9.3.26
libgimp-2_0-0-2.8.18-9.3.26
libgimpui-2_0-0-2.8.18-9.3.26
gimp-plugins-python-debuginfo-2.8.18-9.3.26
gimp-debugsource-2.8.18-9.3.26

noarch
gimp-lang-2.8.18-9.3.26

146086 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:3090-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16837

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3090-1

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-November/003415.html>

SuSE SLES 12 SP3
x86_64
tboot-debuginfo-20160518_1.9.4-7.5.1
tboot-debugsource-20160518_1.9.4-7.5.1
tboot-20160518_1.9.4-7.5.1

SuSE SLES 12 SP2
x86_64
tboot-debuginfo-20160518_1.9.4-7.5.1
tboot-debugsource-20160518_1.9.4-7.5.1
tboot-20160518_1.9.4-7.5.1

146087 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3067-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8116, CVE-2014-8117, CVE-2014-9620, CVE-2014-9621, CVE-2014-9653

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3067-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00071.html>

SuSE Linux 42.2

x86_64

libmagic1-debuginfo-32bit-5.22-7.3.1

libmagic1-32bit-5.22-7.3.1

file-magic-5.22-7.3.1

libmagic1-5.22-7.3.1

file-debuginfo-5.22-7.3.1

file-devel-5.22-7.3.1

file-5.22-7.3.1

libmagic1-debuginfo-5.22-7.3.1

python-magic-5.22-7.3.1

file-debugsource-5.22-7.3.1

i586

file-magic-5.22-7.3.1

libmagic1-5.22-7.3.1

file-debuginfo-5.22-7.3.1

file-devel-5.22-7.3.1

file-5.22-7.3.1

libmagic1-debuginfo-5.22-7.3.1

python-magic-5.22-7.3.1

file-debugsource-5.22-7.3.1

SuSE Linux 42.3

x86_64

file-magic-5.22-10.1

file-5.22-10.1

libmagic1-32bit-5.22-10.1

libmagic1-debuginfo-32bit-5.22-10.1

file-devel-5.22-10.1

libmagic1-5.22-10.1

file-debuginfo-5.22-10.1

libmagic1-debuginfo-5.22-10.1

python-magic-5.22-10.1

file-debugsource-5.22-10.1

i586

file-magic-5.22-10.1

file-5.22-10.1

file-devel-5.22-10.1

libmagic1-5.22-10.1

file-debuginfo-5.22-10.1

libmagic1-debuginfo-5.22-10.1

python-magic-5.22-10.1

file-debugsource-5.22-10.1

146091 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3048-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8116, CVE-2014-8117, CVE-2014-9620, CVE-2014-9621, CVE-2014-9653

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3048-1

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-November/003403.html>

SuSE SLES 12 SP2

x86_64
file-magic-5.22-10.3.1
libmagic1-debuginfo-32bit-5.22-10.3.1
libmagic1-debuginfo-5.22-10.3.1
file-debugsource-5.22-10.3.1
file-debuginfo-5.22-10.3.1
libmagic1-5.22-10.3.1
libmagic1-32bit-5.22-10.3.1
file-5.22-10.3.1

SuSE SLED 12 SP3

x86_64
file-magic-5.22-10.3.1
libmagic1-debuginfo-32bit-5.22-10.3.1
libmagic1-debuginfo-5.22-10.3.1
file-debugsource-5.22-10.3.1
file-debuginfo-5.22-10.3.1
libmagic1-5.22-10.3.1
libmagic1-32bit-5.22-10.3.1
file-5.22-10.3.1

SuSE SLED 12 SP2

x86_64
file-magic-5.22-10.3.1
libmagic1-debuginfo-32bit-5.22-10.3.1
libmagic1-debuginfo-5.22-10.3.1
file-debugsource-5.22-10.3.1
file-debuginfo-5.22-10.3.1
libmagic1-5.22-10.3.1
libmagic1-32bit-5.22-10.3.1
file-5.22-10.3.1

SuSE SLES 12 SP3

x86_64
file-magic-5.22-10.3.1
libmagic1-debuginfo-32bit-5.22-10.3.1
libmagic1-debuginfo-5.22-10.3.1
file-debugsource-5.22-10.3.1
file-debuginfo-5.22-10.3.1
libmagic1-5.22-10.3.1
libmagic1-32bit-5.22-10.3.1
file-5.22-10.3.1

146093 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:3086-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3086-1

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-November/003414.html>

SuSE SLED 12 SP2

x86_64

libdcerpc-at svc0-debuginfo-4.2.4-28.24.1

libdcerpc-at svc0-4.2.4-28.24.1

SuSE SLES 12 SP2

x86_64

libdcerpc-at svc0-debuginfo-4.2.4-28.24.1

libdcerpc-at svc0-4.2.4-28.24.1

146094 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:3104-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3104-1

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-November/003418.html>

SuSE SLED 12 SP2

x86_64

libsamba-util0-32bit-4.4.2-38.14.1

libsamba-passdb0-debuginfo-4.4.2-38.14.1

samba-client-debuginfo-4.4.2-38.14.1

samba-winbind-32bit-4.4.2-38.14.1

libwbclient0-debuginfo-4.4.2-38.14.1

libnetapi0-4.4.2-38.14.1

libsamba-errors0-4.4.2-38.14.1

libdcerpc-binding0-32bit-4.4.2-38.14.1

samba-4.4.2-38.14.1

samba-libs-32bit-4.4.2-38.14.1

libsamba-hostconfig0-debuginfo-4.4.2-38.14.1

libnetapi0-32bit-4.4.2-38.14.1

libsamba-hostconfig0-32bit-4.4.2-38.14.1

libtevent-util0-32bit-4.4.2-38.14.1

libsamba-credentials0-debuginfo-4.4.2-38.14.1

samba-client-debuginfo-32bit-4.4.2-38.14.1

libsamba-errors0-debuginfo-32bit-4.4.2-38.14.1

libdcerpc0-debuginfo-4.4.2-38.14.1

libsamba-passdb0-32bit-4.4.2-38.14.1

samba-libs-debuginfo-4.4.2-38.14.1
libsamba-util0-debuginfo-4.4.2-38.14.1
libdcerpc0-debuginfo-32bit-4.4.2-38.14.1
libndr-standard0-32bit-4.4.2-38.14.1
libsamdb0-4.4.2-38.14.1
libndr-krb5pac0-4.4.2-38.14.1
libsmbclient0-debuginfo-4.4.2-38.14.1
samba-libs-debuginfo-32bit-4.4.2-38.14.1
libnetapi0-debuginfo-32bit-4.4.2-38.14.1
libnetapi0-debuginfo-4.4.2-38.14.1
libwbclient0-4.4.2-38.14.1
libsamba-errors0-32bit-4.4.2-38.14.1
libsamba-credentials0-32bit-4.4.2-38.14.1
libsamba-credentials0-4.4.2-38.14.1
libsmbldap0-debuginfo-4.4.2-38.14.1
libndr0-debuginfo-4.4.2-38.14.1
samba-libs-4.4.2-38.14.1
libsamba-hostconfig0-4.4.2-38.14.1
libndr-standard0-4.4.2-38.14.1
libndr0-32bit-4.4.2-38.14.1
libsmbldap0-4.4.2-38.14.1
samba-debuginfo-4.4.2-38.14.1
libdcerpc-binding0-debuginfo-32bit-4.4.2-38.14.1
libsmbconf0-debuginfo-32bit-4.4.2-38.14.1
libndr-nbt0-debuginfo-32bit-4.4.2-38.14.1
libtevent-util0-4.4.2-38.14.1
libtevent-util0-debuginfo-4.4.2-38.14.1
libndr0-debuginfo-32bit-4.4.2-38.14.1
libsamba-errors0-debuginfo-4.4.2-38.14.1
libndr-krb5pac0-32bit-4.4.2-38.14.1
libsamba-util0-4.4.2-38.14.1
libndr-krb5pac0-debuginfo-32bit-4.4.2-38.14.1
samba-winbind-4.4.2-38.14.1
libsmbconf0-4.4.2-38.14.1
libsmbldap0-32bit-4.4.2-38.14.1
libsmbldap0-debuginfo-32bit-4.4.2-38.14.1
samba-client-32bit-4.4.2-38.14.1
samba-winbind-debuginfo-32bit-4.4.2-38.14.1
libsamba-passsdb0-debuginfo-32bit-4.4.2-38.14.1
libndr-nbt0-4.4.2-38.14.1
libwbclient0-32bit-4.4.2-38.14.1
libsmbconf0-debuginfo-4.4.2-38.14.1
libsamba-credentials0-debuginfo-32bit-4.4.2-38.14.1
libsamdb0-debuginfo-4.4.2-38.14.1
libtevent-util0-debuginfo-32bit-4.4.2-38.14.1
libdcerpc-binding0-4.4.2-38.14.1
libndr-nbt0-32bit-4.4.2-38.14.1
libdcerpc-binding0-debuginfo-4.4.2-38.14.1
libdcerpc0-32bit-4.4.2-38.14.1
samba-winbind-debuginfo-4.4.2-38.14.1
libndr-nbt0-debuginfo-4.4.2-38.14.1
libsamdb0-debuginfo-32bit-4.4.2-38.14.1
libsmbclient0-debuginfo-32bit-4.4.2-38.14.1
libsmbconf0-32bit-4.4.2-38.14.1
libsamba-passsdb0-4.4.2-38.14.1
libsamba-hostconfig0-debuginfo-32bit-4.4.2-38.14.1
samba-client-4.4.2-38.14.1
libwbclient0-debuginfo-32bit-4.4.2-38.14.1
libndr0-4.4.2-38.14.1
libsmbclient0-4.4.2-38.14.1

libsamba-util0-debuginfo-32bit-4.4.2-38.14.1
libsmbclient0-32bit-4.4.2-38.14.1
samba-debugsource-4.4.2-38.14.1
libndr-standard0-debuginfo-4.4.2-38.14.1
libndr-krb5pac0-debuginfo-4.4.2-38.14.1
libndr-standard0-debuginfo-32bit-4.4.2-38.14.1
libsamdb0-32bit-4.4.2-38.14.1
libdcerpc0-4.4.2-38.14.1

noarch
samba-doc-4.4.2-38.14.1

SuSE SLES 12 SP2
noarch
samba-doc-4.4.2-38.14.1

x86_64
libsamba-util0-32bit-4.4.2-38.14.1
libsamba-passdb0-debuginfo-4.4.2-38.14.1
samba-winbind-32bit-4.4.2-38.14.1
libnetapi0-4.4.2-38.14.1
libsamba-errors0-4.4.2-38.14.1
libdcerpc-binding0-32bit-4.4.2-38.14.1
samba-4.4.2-38.14.1
samba-libs-32bit-4.4.2-38.14.1
libwbclient0-debuginfo-32bit-4.4.2-38.14.1
libsamba-hostconfig0-debuginfo-4.4.2-38.14.1
libdcerpc-binding0-debuginfo-4.4.2-38.14.1
libsamba-hostconfig0-32bit-4.4.2-38.14.1
libtevent-util0-32bit-4.4.2-38.14.1
libsamba-credentials0-debuginfo-4.4.2-38.14.1
samba-client-debuginfo-32bit-4.4.2-38.14.1
libsamba-errors0-debuginfo-32bit-4.4.2-38.14.1
libdcerpc0-debuginfo-4.4.2-38.14.1
libsamba-passdb0-32bit-4.4.2-38.14.1
libdcerpc0-debuginfo-32bit-4.4.2-38.14.1
libsamba-util0-debuginfo-4.4.2-38.14.1
libsamdb0-4.4.2-38.14.1
libndr-krb5pac0-4.4.2-38.14.1
libsmbclient0-debuginfo-4.4.2-38.14.1
samba-libs-debuginfo-32bit-4.4.2-38.14.1
libnetapi0-debuginfo-32bit-4.4.2-38.14.1
libnetapi0-debuginfo-4.4.2-38.14.1
libwbclient0-4.4.2-38.14.1
libsamba-errors0-32bit-4.4.2-38.14.1
libsamba-credentials0-32bit-4.4.2-38.14.1
libsamba-credentials0-4.4.2-38.14.1
samba-libs-debuginfo-4.4.2-38.14.1
libndr0-debuginfo-4.4.2-38.14.1
samba-libs-4.4.2-38.14.1
samba-winbind-4.4.2-38.14.1
libndr-standard0-4.4.2-38.14.1
libndr0-32bit-4.4.2-38.14.1
libsmbldap0-4.4.2-38.14.1
samba-debuginfo-4.4.2-38.14.1
libdcerpc-binding0-debuginfo-32bit-4.4.2-38.14.1
libsmbconf0-debuginfo-32bit-4.4.2-38.14.1
libndr-nbt0-debuginfo-32bit-4.4.2-38.14.1
libtevent-util0-4.4.2-38.14.1
libndr0-debuginfo-32bit-4.4.2-38.14.1

libsamba-errors0-debuginfo-4.4.2-38.14.1
libndr-krb5pac0-32bit-4.4.2-38.14.1
libsamba-util0-4.4.2-38.14.1
libndr-krb5pac0-debuginfo-32bit-4.4.2-38.14.1
libndr-standard0-32bit-4.4.2-38.14.1
libsmbconf0-4.4.2-38.14.1
libsamba-hostconfig0-4.4.2-38.14.1
libtevent-util0-debuginfo-4.4.2-38.14.1
libsmbldap0-debuginfo-32bit-4.4.2-38.14.1
samba-winbind-debuginfo-4.4.2-38.14.1
libsmbldap0-debuginfo-4.4.2-38.14.1
samba-winbind-debuginfo-32bit-4.4.2-38.14.1
libsamba-passsdb0-debuginfo-32bit-4.4.2-38.14.1
libndr-nbt0-4.4.2-38.14.1
samba-client-4.4.2-38.14.1
libsmbconf0-debuginfo-4.4.2-38.14.1
libsamba-credentials0-debuginfo-32bit-4.4.2-38.14.1
libsamdb0-debuginfo-4.4.2-38.14.1
libtevent-util0-debuginfo-32bit-4.4.2-38.14.1
libdcerpc-binding0-4.4.2-38.14.1
samba-client-32bit-4.4.2-38.14.1
libsamdb0-32bit-4.4.2-38.14.1
libndr-nbt0-32bit-4.4.2-38.14.1
libsmbldap0-32bit-4.4.2-38.14.1
samba-client-debuginfo-4.4.2-38.14.1
libdcerpc0-32bit-4.4.2-38.14.1
libnetapi0-32bit-4.4.2-38.14.1
libndr-nbt0-debuginfo-4.4.2-38.14.1
libsamdb0-debuginfo-32bit-4.4.2-38.14.1
libsmbclient0-debuginfo-32bit-4.4.2-38.14.1
libsmbconf0-32bit-4.4.2-38.14.1
libsamba-passsdb0-4.4.2-38.14.1
libwbclient0-32bit-4.4.2-38.14.1
libsamba-hostconfig0-debuginfo-32bit-4.4.2-38.14.1
libwbclient0-debuginfo-4.4.2-38.14.1
libndr0-4.4.2-38.14.1
libsmbclient0-4.4.2-38.14.1
libsmbclient0-32bit-4.4.2-38.14.1
samba-debugsource-4.4.2-38.14.1
libndr-standard0-debuginfo-4.4.2-38.14.1
libndr-krb5pac0-debuginfo-4.4.2-38.14.1
libndr-standard0-debuginfo-32bit-4.4.2-38.14.1
libsamba-util0-debuginfo-32bit-4.4.2-38.14.1
libdcerpc0-4.4.2-38.14.1

146095 - SuSE SLES 11 SP4 SUSE-SU-2017:3107-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14798

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3107-1

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-November/003420.html>

SuSE SLES 11 SP4
noarch
postgresql-init-9.4-0.5.3.1

146097 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3095-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-8911

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3095-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00077.html>

SuSE Linux 42.2
x86_64
tnef-debuginfo-1.4.15-5.3.1
tnef-debugsource-1.4.15-5.3.1
tnef-1.4.15-5.3.1

i586
tnef-debuginfo-1.4.15-5.3.1
tnef-debugsource-1.4.15-5.3.1
tnef-1.4.15-5.3.1

SuSE Linux 42.3
x86_64
tnef-debugsource-1.4.15-8.1
tnef-debuginfo-1.4.15-8.1
tnef-1.4.15-8.1

i586
tnef-debugsource-1.4.15-8.1
tnef-debuginfo-1.4.15-8.1
tnef-1.4.15-8.1

146098 - SuSE Linux 42.2 openSUSE-SU-2017:3097-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15923

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3097-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00079.html>

SuSE Linux 42.2

i586

konversation-1.6.2-2.3.1

konversation-debugsource-1.6.2-2.3.1

konversation-debuginfo-1.6.2-2.3.1

noarch

konversation-lang-1.6.2-2.3.1

x86_64

konversation-1.6.2-2.3.1

konversation-debugsource-1.6.2-2.3.1

konversation-debuginfo-1.6.2-2.3.1

146099 - SuSE Linux 42.3 openSUSE-SU-2017:3099-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15923

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3099-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00081.html>

SuSE Linux 42.3

i586

konversation-debugsource-1.7.4-3.1

konversation-debuginfo-1.7.4-3.1

konversation-1.7.4-3.1

noarch

konversation-lang-1.7.4-3.1

x86_64

konversation-debugsource-1.7.4-3.1

konversation-debuginfo-1.7.4-3.1

konversation-1.7.4-3.1

146100 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3096-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16667

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3096-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00078.html>

SuSE Linux 42.2

noarch
backintime-qt4-1.1.20-3.6.1
backintime-lang-1.1.20-3.6.1
backintime-1.1.20-3.6.1

SuSE Linux 42.3

noarch
backintime-1.1.20-6.1
backintime-lang-1.1.20-6.1
backintime-qt4-1.1.20-6.1

146101 - SuSE SLES 11 SP4 SUSE-SU-2017:3078-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8184, CVE-2017-15101

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3078-1

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-November/003411.html>

SuSE SLES 11 SP4

i586
python-louis-1.7.0-1.3.6.1
liblouis0-1.7.0-1.3.6.1
liblouis-1.7.0-1.3.6.1

x86_64

python-louis-1.7.0-1.3.6.1
liblouis0-1.7.0-1.3.6.1
liblouis-1.7.0-1.3.6.1

146103 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3100-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16837

Description

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

openSUSE-SU-2017:3100-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00082.html>

SuSE Linux 42.2

x86_64

tboot-debuginfo-20170711_1.9.6-4.3.1

tboot-20170711_1.9.6-4.3.1

tboot-debugsource-20170711_1.9.6-4.3.1

i586

tboot-debuginfo-20170711_1.9.6-4.3.1

tboot-20170711_1.9.6-4.3.1

tboot-debugsource-20170711_1.9.6-4.3.1

SuSE Linux 42.3

x86_64

tboot-20170711_1.9.6-7.1

tboot-debuginfo-20170711_1.9.6-7.1

tboot-debugsource-20170711_1.9.6-7.1

i586

tboot-20170711_1.9.6-7.1

tboot-debuginfo-20170711_1.9.6-7.1

tboot-debugsource-20170711_1.9.6-7.1

146106 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3108-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-7826, CVE-2017-7828, CVE-2017-7830

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3108-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00085.html>

SuSE Linux 42.2

x86_64

MozillaThunderbird-buildsymbols-52.5.0-41.21.1

MozillaThunderbird-52.5.0-41.21.1

MozillaThunderbird-debuginfo-52.5.0-41.21.1

MozillaThunderbird-translations-common-52.5.0-41.21.1

MozillaThunderbird-devel-52.5.0-41.21.1

MozillaThunderbird-translations-other-52.5.0-41.21.1

MozillaThunderbird-debugsource-52.5.0-41.21.1

SuSE Linux 42.3

x86_64
MozillaThunderbird-buildsymbols-52.5.0-50.1
MozillaThunderbird-52.5.0-50.1
MozillaThunderbird-translations-common-52.5.0-50.1
MozillaThunderbird-translations-other-52.5.0-50.1
MozillaThunderbird-devel-52.5.0-50.1
MozillaThunderbird-debuginfo-52.5.0-50.1
MozillaThunderbird-debugsource-52.5.0-50.1

146107 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3054-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15864, CVE-2017-16664

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3054-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00066.html>

SuSE Linux 42.2
noarch
otrs-3.3.20-5.11.1
otrs-doc-3.3.20-5.11.1
otrs-itsm-3.3.14-5.11.1

SuSE Linux 42.3
noarch
otrs-doc-3.3.20-14.1
otrs-3.3.20-14.1
otrs-itsm-3.3.14-14.1

160327 - CentOS 7 CESA-2017-3260 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
CESA-2017-3260

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-November/022631.html>

CentOS 7
i686
samba-client-libs-4.6.2-12.el7_4

samba-winbind-modules-4.6.2-12.el7_4
samba-test-libs-4.6.2-12.el7_4
libwbclient-devel-4.6.2-12.el7_4
libwbclient-4.6.2-12.el7_4
samba-libs-4.6.2-12.el7_4
samba-devel-4.6.2-12.el7_4
libsmbclient-devel-4.6.2-12.el7_4
libsmbclient-4.6.2-12.el7_4

noarch
samba-pidl-4.6.2-12.el7_4
samba-common-4.6.2-12.el7_4

x86_64
libwbclient-devel-4.6.2-12.el7_4
samba-test-libs-4.6.2-12.el7_4
samba-winbind-clients-4.6.2-12.el7_4
samba-libs-4.6.2-12.el7_4
samba-devel-4.6.2-12.el7_4
libsmbclient-4.6.2-12.el7_4
samba-dc-4.6.2-12.el7_4
libsmbclient-devel-4.6.2-12.el7_4
samba-4.6.2-12.el7_4
samba-winbind-krb5-locator-4.6.2-12.el7_4
samba-krb5-printing-4.6.2-12.el7_4
samba-python-4.6.2-12.el7_4
samba-test-4.6.2-12.el7_4
samba-vfs-glusterfs-4.6.2-12.el7_4
ctdb-4.6.2-12.el7_4
libwbclient-4.6.2-12.el7_4
samba-common-tools-4.6.2-12.el7_4
samba-dc-libs-4.6.2-12.el7_4
samba-winbind-modules-4.6.2-12.el7_4
samba-common-libs-4.6.2-12.el7_4
samba-client-libs-4.6.2-12.el7_4
ctdb-tests-4.6.2-12.el7_4
samba-winbind-4.6.2-12.el7_4
samba-client-4.6.2-12.el7_4

163498 - Oracle Enterprise Linux ELSA-2017-3260 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
ELSA-2017-3260

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-November/007355.html>

OEL7
x86_64
ctdb-4.6.2-12.el7_4

libwbclient-devel-4.6.2-12.el7_4
samba-common-4.6.2-12.el7_4
samba-winbind-clients-4.6.2-12.el7_4
samba-libs-4.6.2-12.el7_4
samba-devel-4.6.2-12.el7_4
libsmbclient-4.6.2-12.el7_4
samba-dc-4.6.2-12.el7_4
libsmbclient-devel-4.6.2-12.el7_4
samba-4.6.2-12.el7_4
samba-winbind-krb5-locator-4.6.2-12.el7_4
samba-winbind-4.6.2-12.el7_4
samba-krb5-printing-4.6.2-12.el7_4
samba-python-4.6.2-12.el7_4
samba-test-4.6.2-12.el7_4
samba-vfs-glusterfs-4.6.2-12.el7_4
samba-dc-libs-4.6.2-12.el7_4
libwbclient-4.6.2-12.el7_4
samba-common-tools-4.6.2-12.el7_4
samba-winbind-modules-4.6.2-12.el7_4
samba-common-libs-4.6.2-12.el7_4
ctdb-tests-4.6.2-12.el7_4
samba-client-libs-4.6.2-12.el7_4
samba-test-libs-4.6.2-12.el7_4
samba-pidl-4.6.2-12.el7_4
samba-client-4.6.2-12.el7_4

175288 - Scientific Linux Security ERRATA Important: samba on SL7.x x86_64 (1711-1601)

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

Risk Level: High

CVE: CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: samba on SL7.x x86_64 (1711-1601)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1711&L=scientific-linux-errata&F=&S=&P=1601>

SL7

x86_64

libwbclient-devel-4.6.2-12.el7_4
samba-devel-4.6.2-12.el7_4
libsmbclient-4.6.2-12.el7_4
samba-4.6.2-12.el7_4
libsmbclient-devel-4.6.2-12.el7_4
samba-libs-4.6.2-12.el7_4
samba-winbind-krb5-locator-4.6.2-12.el7_4
samba-dc-4.6.2-12.el7_4
samba-debuginfo-4.6.2-12.el7_4
samba-krb5-printing-4.6.2-12.el7_4
samba-winbind-modules-4.6.2-12.el7_4
samba-test-4.6.2-12.el7_4
samba-vfs-glusterfs-4.6.2-12.el7_4
samba-winbind-clients-4.6.2-12.el7_4

libwbclient-4.6.2-12.el7_4
samba-common-tools-4.6.2-12.el7_4
samba-dc-libs-4.6.2-12.el7_4
samba-python-4.6.2-12.el7_4
samba-common-libs-4.6.2-12.el7_4
samba-client-libs-4.6.2-12.el7_4
samba-test-libs-4.6.2-12.el7_4
samba-winbind-4.6.2-12.el7_4
samba-client-4.6.2-12.el7_4

noarch
samba-pidl-4.6.2-12.el7_4
samba-common-4.6.2-12.el7_4

182527 - FreeBSD salt Multiple Vulnerabilities (50127e44-7b88-4ade-8e12-5d57320823f1)

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

Risk Level: High

CVE: CVE-2017-14695, CVE-2017-14696

Description

The scan detected that the host is missing the following update:
salt -- multiple vulnerabilities (50127e44-7b88-4ade-8e12-5d57320823f1)

Observation

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

<http://www.vuxml.org/freebsd/50127e44-7b88-4ade-8e12-5d57320823f1.html>

Affected packages:

py27-salt < 2016.11.8
py32-salt < 2016.11.8
py33-salt < 2016.11.8
py34-salt < 2016.11.8
py35-salt < 2016.11.8
py36-salt < 2016.11.8
2017.7.0 <= py27-salt < 2017.7.2
2017.7.0 <= py32-salt < 2017.7.2
2017.7.0 <= py33-salt < 2017.7.2
2017.7.0 <= py34-salt < 2017.7.2
2017.7.0 <= py35-salt < 2017.7.2
2017.7.0 <= py36-salt < 2017.7.2

185990 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3494-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10672

Description

The scan detected that the host is missing the following update:
USN-3494-1

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-November/004162.html>

Ubuntu 16.04

libxml-libxml-perl_2.0123+dfsg-1ubuntu0.1

Ubuntu 14.04

libxml-libxml-perl_2.0108+dfsg-1ubuntu0.2

Ubuntu 17.04

libxml-libxml-perl_2.0128+dfsg-1ubuntu0.1

Ubuntu 17.10

libxml-libxml-perl_2.0128+dfsg-3ubuntu0.1

185992 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3492-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-3885, CVE-2015-8366, CVE-2015-8367, CVE-2017-13735, CVE-2017-14265, CVE-2017-14348, CVE-2017-14608, CVE-2017-6886, CVE-2017-6887

Description

The scan detected that the host is missing the following update:
USN-3492-1

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-November/004158.html>

Ubuntu 16.04

libraw15_0.17.1-1ubuntu0.1

Ubuntu 14.04

libraw9_0.15.4-1ubuntu0.1

Ubuntu 17.04

libraw16_0.18.1-1ubuntu0.1

Ubuntu 17.10

libraw16_0.18.2-2ubuntu0.1

192996 - Fedora Linux 25 FEDORA-2017-f1535b86fa Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12629

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f1535b86fa

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/2017/11/?count=200&page=1>

Fedora Core 25

lucene4-4.10.4-11.fc25

22772 - (SB10210) Network Security Manager Improper Authorization Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-8029

Description

A vulnerability is present in some versions of McAfee Network Security Manager.

Observation

McAfee Network Security Manager is a next-generation intrusion prevention system (IPS).

A vulnerability is present in some versions of McAfee Network Security Manager. The flaw lies in the web interface. Successful exploitation of this vulnerability could allow a malicious user to obtain elevated privileges within this software context. Exploitation requires an authenticated user to send a crafted HTTP request to obtain elevated privileges.

96039 - Fedora Linux 26 FEDORA-2017-4d5618a962 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13788, CVE-2017-13798, CVE-2017-13803

Description

The scan detected that the host is missing the following update:
FEDORA-2017-4d5618a962

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/2017/11/?count=200&page=1>

Fedora Core 26

webkitgtk4-2.18.3-1.fc26

96042 - Fedora Linux 25 FEDORA-2017-077334783e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13788, CVE-2017-13798, CVE-2017-13803

Description

The scan detected that the host is missing the following update:
FEDORA-2017-077334783e

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/2017/11/?count=200&page=1>

Fedora Core 25

webkitgtk4-2.18.3-1.fc25

130955 - Debian Linux 9.0 DSA-4049-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15186, CVE-2017-15672, CVE-2017-16840

Description

The scan detected that the host is missing the following update:
DSA-4049-1

Observation

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

<http://www.debian.org/security/2017/dsa-4049>

Debian 9.0

all

ffmpeg_7:3.2.9-1~deb9u1

130957 - Debian Linux 8.0 DSA-4048-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10274, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

The scan detected that the host is missing the following update:
DSA-4048-1

Observation

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

<http://www.debian.org/security/2017/dsa-4048>

Debian 8.0

all

openjdk-7-dbg_7u151-2.6.11-2~deb8u1

icedtea-7-jre-jamvm_7u151-2.6.11-2~deb8u1

openjdk-7-jre-zero_7u151-2.6.11-2~deb8u1

openjdk-7-demo_7u151-2.6.11-2~deb8u1

openjdk-7-jre_7u151-2.6.11-2~deb8u1

openjdk-7-jre-headless_7u151-2.6.11-2~deb8u1

openjdk-7-doc_7u151-2.6.11-2~deb8u1

openjdk-7-jdk_7u151-2.6.11-2~deb8u1

openjdk-7-jre-lib_7u151-2.6.11-2~deb8u1

openjdk-7-source_7u151-2.6.11-2~deb8u1

141780 - Red Hat Enterprise Linux RHSA-2017-3264 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10165, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, CVE-2017-10309, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

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

RHSA-2017-3264

Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2017-November/msg00032.html>

RHEL7D

x86_64

java-1.8.0-ibm-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-plugin-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-jdbc-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-devel-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-demo-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-src-1.8.0.5.5-1jpp.2.el7

RHEL7S

x86_64

java-1.8.0-ibm-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-plugin-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-jdbc-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-devel-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-demo-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-src-1.8.0.5.5-1jpp.2.el7

RHEL7WS

x86_64

java-1.8.0-ibm-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-plugin-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-jdbc-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-devel-1.8.0.5.5-1jpp.2.el7

java-1.8.0-ibm-demo-1.8.0.5.5-1jpp.2.el7

141781 - Red Hat Enterprise Linux RHSA-2017-3268 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10165, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

The scan detected that the host is missing the following update:
RHSA-2017-3268

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2017-November/msg00035.html>

RHEL7S

x86_64

java-1.7.1-ibm-devel-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-jdbc-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-plugin-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-demo-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-src-1.7.1.4.15-1jpp.2.el7

RHEL6S

i386

java-1.7.1-ibm-plugin-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-src-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-demo-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-jdbc-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-devel-1.7.1.4.15-1jpp.3.el6_9

x86_64

java-1.7.1-ibm-plugin-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-src-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-demo-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-jdbc-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-devel-1.7.1.4.15-1jpp.3.el6_9

RHEL6WS

x86_64

java-1.7.1-ibm-plugin-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-src-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-demo-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-jdbc-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-devel-1.7.1.4.15-1jpp.3.el6_9

i386

java-1.7.1-ibm-plugin-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-src-1.7.1.4.15-1jpp.3.el6_9

java-1.7.1-ibm-demo-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-jdbc-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-devel-1.7.1.4.15-1jpp.3.el6_9

RHEL7D

x86_64
java-1.7.1-ibm-devel-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-jdbc-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-plugin-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-demo-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-src-1.7.1.4.15-1jpp.2.el7

RHEL6D

x86_64
java-1.7.1-ibm-plugin-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-src-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-demo-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-jdbc-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-devel-1.7.1.4.15-1jpp.3.el6_9

i386

java-1.7.1-ibm-plugin-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-src-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-demo-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-jdbc-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-1.7.1.4.15-1jpp.3.el6_9
java-1.7.1-ibm-devel-1.7.1.4.15-1jpp.3.el6_9

RHEL7WS

x86_64
java-1.7.1-ibm-devel-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-jdbc-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-plugin-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-demo-1.7.1.4.15-1jpp.2.el7
java-1.7.1-ibm-src-1.7.1.4.15-1jpp.2.el7

141784 - Red Hat Enterprise Linux RHSA-2017-3263 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000257

Description

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

RHSA-2017-3263

Observation

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

For more information see:

<http://www.redhat.com/archives/rhsa-announce/2017-November/msg00031.html>

RHEL7D

x86_64

libcurl-devel-7.29.0-42.el7_4.1
curl-debuginfo-7.29.0-42.el7_4.1
libcurl-7.29.0-42.el7_4.1
curl-7.29.0-42.el7_4.1

RHEL7S

x86_64
libcurl-devel-7.29.0-42.el7_4.1
curl-debuginfo-7.29.0-42.el7_4.1
libcurl-7.29.0-42.el7_4.1
curl-7.29.0-42.el7_4.1

RHEL7WS

x86_64
libcurl-devel-7.29.0-42.el7_4.1
curl-debuginfo-7.29.0-42.el7_4.1
libcurl-7.29.0-42.el7_4.1
curl-7.29.0-42.el7_4.1

141785 - Red Hat Enterprise Linux RHSA-2017-3267 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10165, CVE-2017-10281, CVE-2017-10285, CVE-2017-10295, CVE-2017-10309, CVE-2017-10345, CVE-2017-10346, CVE-2017-10347, CVE-2017-10348, CVE-2017-10349, CVE-2017-10350, CVE-2017-10355, CVE-2017-10356, CVE-2017-10357, CVE-2017-10388

Description

The scan detected that the host is missing the following update:
RHSA-2017-3267

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2017-November/msg00034.html>

RHEL6D

x86_64
java-1.8.0-ibm-devel-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-src-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-demo-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-jdbc-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-plugin-1.8.0.5.5-1jpp.1.el6_9

i386

java-1.8.0-ibm-devel-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-src-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-demo-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-jdbc-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-plugin-1.8.0.5.5-1jpp.1.el6_9

RHEL6S

i386
java-1.8.0-ibm-devel-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-src-1.8.0.5.5-1jpp.1.el6_9

java-1.8.0-ibm-demo-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-jdbc-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-plugin-1.8.0.5.5-1jpp.1.el6_9

x86_64

java-1.8.0-ibm-devel-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-src-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-demo-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-jdbc-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-plugin-1.8.0.5.5-1jpp.1.el6_9

RHEL6WS

x86_64

java-1.8.0-ibm-devel-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-src-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-demo-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-jdbc-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-plugin-1.8.0.5.5-1jpp.1.el6_9

i386

java-1.8.0-ibm-devel-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-src-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-demo-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-jdbc-1.8.0.5.5-1jpp.1.el6_9
java-1.8.0-ibm-plugin-1.8.0.5.5-1jpp.1.el6_9

146089 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:3039-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12617, CVE-2017-5664, CVE-2017-7674

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3039-1

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-November/003401.html>

SuSE SLES 12 SP3

noarch

tomcat-admin-webapps-8.0.43-29.5.1
tomcat-el-3_0-api-8.0.43-29.5.1
tomcat-webapps-8.0.43-29.5.1
tomcat-javadoc-8.0.43-29.5.1
tomcat-jsp-2_3-api-8.0.43-29.5.1
tomcat-docs-webapp-8.0.43-29.5.1
tomcat-servlet-3_1-api-8.0.43-29.5.1
tomcat-lib-8.0.43-29.5.1
tomcat-8.0.43-29.5.1

SuSE SLES 12 SP2
noarch
tomcat-admin-webapps-8.0.43-29.5.1
tomcat-el-3_0-api-8.0.43-29.5.1
tomcat-webapps-8.0.43-29.5.1
tomcat-javadoc-8.0.43-29.5.1
tomcat-jsp-2_3-api-8.0.43-29.5.1
tomcat-docs-webapp-8.0.43-29.5.1
tomcat-servlet-3_1-api-8.0.43-29.5.1
tomcat-lib-8.0.43-29.5.1
tomcat-8.0.43-29.5.1

146090 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3069-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12617, CVE-2017-5664, CVE-2017-7674

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3069-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00073.html>

SuSE Linux 42.2
noarch
tomcat-el-3_0-api-8.0.43-6.13.1
tomcat-jsp-2_3-api-8.0.43-6.13.1
tomcat-servlet-3_1-api-8.0.43-6.13.1
tomcat-admin-webapps-8.0.43-6.13.1
tomcat-embed-8.0.43-6.13.1
tomcat-docs-webapp-8.0.43-6.13.1
tomcat-jsvc-8.0.43-6.13.1
tomcat-lib-8.0.43-6.13.1
tomcat-8.0.43-6.13.1
tomcat-javadoc-8.0.43-6.13.1
tomcat-webapps-8.0.43-6.13.1

SuSE Linux 42.3
noarch
tomcat-webapps-8.0.43-9.1
tomcat-8.0.43-9.1
tomcat-servlet-3_1-api-8.0.43-9.1
tomcat-docs-webapp-8.0.43-9.1
tomcat-javadoc-8.0.43-9.1
tomcat-jsvc-8.0.43-9.1
tomcat-embed-8.0.43-9.1
tomcat-lib-8.0.43-9.1
tomcat-jsp-2_3-api-8.0.43-9.1
tomcat-el-3_0-api-8.0.43-9.1
tomcat-admin-webapps-8.0.43-9.1

146102 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3101-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12837, CVE-2017-12883, CVE-2017-6512

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2017:3101-1

Observation

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

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00083.html>

SuSE Linux 42.2

i586

perl-debuginfo-5.18.2-6.3.1

perl-debugsource-5.18.2-6.3.1

perl-base-5.18.2-6.3.1

perl-base-debuginfo-5.18.2-6.3.1

perl-5.18.2-6.3.1

noarch

perl-doc-5.18.2-6.3.1

x86_64

perl-debuginfo-32bit-5.18.2-6.3.1

perl-5.18.2-6.3.1

perl-base-32bit-5.18.2-6.3.1

perl-debuginfo-5.18.2-6.3.1

perl-debugsource-5.18.2-6.3.1

perl-32bit-5.18.2-6.3.1

perl-base-debuginfo-32bit-5.18.2-6.3.1

perl-base-5.18.2-6.3.1

perl-base-debuginfo-5.18.2-6.3.1

SuSE Linux 42.3

i586

perl-debugsource-5.18.2-9.1

perl-base-debuginfo-5.18.2-9.1

perl-debuginfo-5.18.2-9.1

perl-base-5.18.2-9.1

perl-5.18.2-9.1

noarch

perl-doc-5.18.2-9.1

x86_64

perl-debugsource-5.18.2-9.1

perl-base-debuginfo-32bit-5.18.2-9.1

perl-base-32bit-5.18.2-9.1

perl-32bit-5.18.2-9.1

perl-base-debuginfo-5.18.2-9.1

perl-debuginfo-5.18.2-9.1

perl-5.18.2-9.1

perl-debuginfo-32bit-5.18.2-9.1

perl-base-5.18.2-9.1

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

Risk Level: Medium

CVE: CVE-2017-12837, CVE-2017-12883, CVE-2017-6512

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3092-1

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-November/003416.html>

SuSE SLES 12 SP2

noarch
perl-doc-5.18.2-12.3.1

x86_64
perl-base-debuginfo-5.18.2-12.3.1
perl-debuginfo-5.18.2-12.3.1
perl-32bit-5.18.2-12.3.1
perl-debugsource-5.18.2-12.3.1
perl-debuginfo-32bit-5.18.2-12.3.1
perl-base-5.18.2-12.3.1
perl-5.18.2-12.3.1

SuSE SLED 12 SP3

x86_64
perl-base-debuginfo-5.18.2-12.3.1
perl-debuginfo-5.18.2-12.3.1
perl-32bit-5.18.2-12.3.1
perl-debugsource-5.18.2-12.3.1
perl-debuginfo-32bit-5.18.2-12.3.1
perl-base-5.18.2-12.3.1
perl-5.18.2-12.3.1

noarch
perl-doc-5.18.2-12.3.1

SuSE SLED 12 SP2

x86_64
perl-base-debuginfo-5.18.2-12.3.1
perl-debuginfo-5.18.2-12.3.1
perl-32bit-5.18.2-12.3.1
perl-debugsource-5.18.2-12.3.1
perl-debuginfo-32bit-5.18.2-12.3.1
perl-base-5.18.2-12.3.1
perl-5.18.2-12.3.1

noarch
perl-doc-5.18.2-12.3.1

SuSE SLES 12 SP3

noarch
perl-doc-5.18.2-12.3.1

x86_64
perl-base-debuginfo-5.18.2-12.3.1
perl-debuginfo-5.18.2-12.3.1
perl-32bit-5.18.2-12.3.1
perl-debugsource-5.18.2-12.3.1
perl-debuginfo-32bit-5.18.2-12.3.1
perl-base-5.18.2-12.3.1
perl-5.18.2-12.3.1

160326 - CentOS 7 CESA-2017-3263 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000257

Description

The scan detected that the host is missing the following update:
CESA-2017-3263

Observation

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

<http://lists.centos.org/pipermail/centos-announce/2017-November/022630.html>

CentOS 7
x86_64
libcurl-devel-7.29.0-42.el7_4.1
curl-7.29.0-42.el7_4.1
libcurl-7.29.0-42.el7_4.1

i686
libcurl-7.29.0-42.el7_4.1
libcurl-devel-7.29.0-42.el7_4.1

163499 - Oracle Enterprise Linux ELSA-2017-3263 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000257

Description

The scan detected that the host is missing the following update:
ELSA-2017-3263

Observation

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

<http://oss.oracle.com/pipermail/el-errata/2017-November/007356.html>

OEL7
x86_64
libcurl-devel-7.29.0-42.el7_4.1
curl-7.29.0-42.el7_4.1
libcurl-7.29.0-42.el7_4.1

175289 - Scientific Linux Security ERRATA Moderate: curl on SL7.x x86_64 (1711-1942)

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

Risk Level: Medium

CVE: CVE-2017-1000257

Description

The scan detected that the host is missing the following update:
Security ERRATA Moderate: curl on SL7.x x86_64 (1711-1942)

Observation

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

<https://listserv.fnal.gov/scripts/wa.exe?A2=ind1711&L=scientific-linux-errata&F=&S=&P=1942>

SL7

x86_64

libcurl-devel-7.29.0-42.el7_4.1

curl-debuginfo-7.29.0-42.el7_4.1

libcurl-7.29.0-42.el7_4.1

curl-7.29.0-42.el7_4.1

192998 - Fedora Linux 25 FEDORA-2017-580f91f6b0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5092, CVE-2017-5093, CVE-2017-5095, CVE-2017-5097, CVE-2017-5099, CVE-2017-5102, CVE-2017-5103, CVE-2017-5107, CVE-2017-5112, CVE-2017-5114, CVE-2017-5117, CVE-2017-5118

Description

The scan detected that the host is missing the following update:
FEDORA-2017-580f91f6b0

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/2017/11/?count=200&page=2>

Fedora Core 25

qt5-qtwebengine-5.9.2-2.fc25

22777 - IBM WebSphere Application Server Liberty Information Disclosure Vulnerability (swg22008707)

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

Risk Level: Medium

CVE: CVE-2013-6440

Description

An XML external entity (XEE) vulnerability is present in some versions of IBM WebSphere Application Server Liberty Profile.

Observation

IBM WebSphere Application Server Liberty Profile is a server engine for Java EE Web applications.

An XML external entity (XEE) vulnerability is present in some versions of IBM WebSphere Application Server Liberty Profile. The flaw lies in the XML parser. Exploitation could allow a malicious user to obtain sensitive information. Exploitation requires the user to be persuaded to open a specially crafted XML document that contains external entity references.

22793 - IBM HTTP Server Multiple Vulnerabilities (swg22009782)

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

Risk Level: Medium

CVE: CVE-2017-12618, CVE-2017-9798

Description

Multiple vulnerabilities are present in some versions of IBM HTTP Server.

Observation

IBM HTTP Server is an Apache-based web server.

Multiple vulnerabilities are present in some versions of IBM HTTP Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information, or cause denial of service condition.

96038 - Fedora Linux 26 FEDORA-2017-4862a3bfb1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15906

Description

The scan detected that the host is missing the following update:
FEDORA-2017-4862a3bfb1

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/2017/11/?count=200&page=1>

Fedora Core 26

openssh-7.5p1-4.fc26

141786 - Red Hat Enterprise Linux RHSA-2017-3265 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-10155, CVE-2017-10227, CVE-2017-10268, CVE-2017-10276, CVE-2017-10279, CVE-2017-10283, CVE-2017-10286, CVE-2017-10294, CVE-2017-10314, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384

Description

The scan detected that the host is missing the following update:
RHSA-2017-3265

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2017-November/msg00033.html>

RHEL6_7S

x86_64

rh-mysql56-mysql-config-5.6.38-1.el6
rh-mysql56-mysql-test-5.6.38-1.el6
rh-mysql56-mysql-common-5.6.38-1.el6
rh-mysql56-mysql-5.6.38-1.el6
rh-mysql56-mysql-errmsg-5.6.38-1.el6
rh-mysql56-mysql-server-5.6.38-1.el6
rh-mysql56-mysql-bench-5.6.38-1.el6
rh-mysql56-mysql-devel-5.6.38-1.el6
rh-mysql56-mysql-debuginfo-5.6.38-1.el6

RHEL6S

x86_64

rh-mysql56-mysql-config-5.6.38-1.el6
rh-mysql56-mysql-test-5.6.38-1.el6
rh-mysql56-mysql-common-5.6.38-1.el6
rh-mysql56-mysql-5.6.38-1.el6
rh-mysql56-mysql-errmsg-5.6.38-1.el6
rh-mysql56-mysql-server-5.6.38-1.el6
rh-mysql56-mysql-bench-5.6.38-1.el6
rh-mysql56-mysql-devel-5.6.38-1.el6
rh-mysql56-mysql-debuginfo-5.6.38-1.el6

RHEL6WS

x86_64

rh-mysql56-mysql-config-5.6.38-1.el6
rh-mysql56-mysql-test-5.6.38-1.el6
rh-mysql56-mysql-common-5.6.38-1.el6
rh-mysql56-mysql-5.6.38-1.el6
rh-mysql56-mysql-errmsg-5.6.38-1.el6
rh-mysql56-mysql-server-5.6.38-1.el6
rh-mysql56-mysql-bench-5.6.38-1.el6
rh-mysql56-mysql-devel-5.6.38-1.el6
rh-mysql56-mysql-debuginfo-5.6.38-1.el6

RHEL7S

x86_64

rh-mysql56-mysql-debuginfo-5.6.38-1.el7
rh-mysql56-mysql-bench-5.6.38-1.el7
rh-mysql56-mysql-server-5.6.38-1.el7
rh-mysql56-mysql-errmsg-5.6.38-1.el7
rh-mysql56-mysql-test-5.6.38-1.el7
rh-mysql56-mysql-5.6.38-1.el7
rh-mysql56-mysql-common-5.6.38-1.el7
rh-mysql56-mysql-config-5.6.38-1.el7
rh-mysql56-mysql-devel-5.6.38-1.el7

RHEL7WS

x86_64

rh-mysql56-mysql-debuginfo-5.6.38-1.el7
rh-mysql56-mysql-bench-5.6.38-1.el7
rh-mysql56-mysql-server-5.6.38-1.el7

rh-mysql56-mysql-errmsg-5.6.38-1.el7
rh-mysql56-mysql-test-5.6.38-1.el7
rh-mysql56-mysql-5.6.38-1.el7
rh-mysql56-mysql-common-5.6.38-1.el7
rh-mysql56-mysql-config-5.6.38-1.el7
rh-mysql56-mysql-devel-5.6.38-1.el7

146088 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3064-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10221, CVE-2016-8728, CVE-2016-8729, CVE-2017-7976

Description

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

openSUSE-SU-2017:3064-1

Observation

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

For more information see:

<http://lists.opensuse.org/opensuse-updates/2017-11/msg00068.html>

SuSE Linux 42.2

x86_64

mupdf-1.11-13.3.1

mupdf-devel-static-1.11-13.3.1

i586

mupdf-1.11-13.3.1

mupdf-devel-static-1.11-13.3.1

SuSE Linux 42.3

x86_64

mupdf-devel-static-1.11-16.1

mupdf-1.11-16.1

i586

mupdf-devel-static-1.11-16.1

mupdf-1.11-16.1

192987 - Fedora Linux 26 FEDORA-2017-dbec196dd8 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3735, CVE-2017-3736

Description

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

FEDORA-2017-dbec196dd8

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/2017/11/?count=200&page=1>

Fedora Core 26

openssl-1.1.0g-1.fc26

192988 - Fedora Linux 25 FEDORA-2017-55a3247cfd Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3735, CVE-2017-3736

Description

The scan detected that the host is missing the following update:
FEDORA-2017-55a3247cfd

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/2017/11/?count=200&page=1>

Fedora Core 25

openssl-1.0.2m-1.fc25

192990 - Fedora Linux 26 FEDORA-2017-df3032c978 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16227

Description

The scan detected that the host is missing the following update:
FEDORA-2017-df3032c978

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/2017/11/?count=200&page=1>

Fedora Core 26

quagga-1.2.2-1.fc26

22783 - (K99998454) F5 BIG-IP Icontrol REST Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2016-5021

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 iControl REST service. Successful exploitation could allow an attacker to obtain sensitive information.

96049 - Fedora Linux 26 FEDORA-2017-742be0e59c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15298

Description

The scan detected that the host is missing the following update:
FEDORA-2017-742be0e59c

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/2017/11/?count=200&page=1>

Fedora Core 26

git-2.13.6-2.fc26

146096 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3047-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12176, CVE-2017-12177, CVE-2017-12178, CVE-2017-12179, CVE-2017-12180, CVE-2017-12181, CVE-2017-12182, CVE-2017-12183, CVE-2017-12184, CVE-2017-12185, CVE-2017-12186, CVE-2017-12187, CVE-2017-13721, CVE-2017-13723

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3047-1

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-November/003402.html>

SuSE SLES 12 SP2

x86_64

xorg-x11-server-extra-7.6_1.18.3-76.15.2

xorg-x11-server-extra-debuginfo-7.6_1.18.3-76.15.2

xorg-x11-server-debuginfo-7.6_1.18.3-76.15.2

xorg-x11-server-debugsource-7.6_1.18.3-76.15.2

xorg-x11-server-7.6_1.18.3-76.15.2

SuSE SLED 12 SP3

x86_64

xorg-x11-server-extra-7.6_1.18.3-76.15.2

xorg-x11-server-extra-debuginfo-7.6_1.18.3-76.15.2
xorg-x11-server-debuginfo-7.6_1.18.3-76.15.2
xorg-x11-server-debugsource-7.6_1.18.3-76.15.2
xorg-x11-server-7.6_1.18.3-76.15.2

SuSE SLED 12 SP2

x86_64
xorg-x11-server-extra-7.6_1.18.3-76.15.2
xorg-x11-server-extra-debuginfo-7.6_1.18.3-76.15.2
xorg-x11-server-debuginfo-7.6_1.18.3-76.15.2
xorg-x11-server-debugsource-7.6_1.18.3-76.15.2
xorg-x11-server-7.6_1.18.3-76.15.2

SuSE SLES 12 SP3

x86_64
xorg-x11-server-extra-7.6_1.18.3-76.15.2
xorg-x11-server-extra-debuginfo-7.6_1.18.3-76.15.2
xorg-x11-server-debuginfo-7.6_1.18.3-76.15.2
xorg-x11-server-debugsource-7.6_1.18.3-76.15.2
xorg-x11-server-7.6_1.18.3-76.15.2

192985 - Fedora Linux 25 FEDORA-2017-ed565f9ed0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9216

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ed565f9ed0

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/2017/11/?count=200&page=1>

Fedora Core 25

jbig2dec-0.14-1.fc25

88900 - Slackware Linux 14.0, 14.1, 14.2 SSA:2017-332-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
SSA:2017-332-01

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.481297>

Slackware 14.0
x86_64
samba-4.4.16-x86_64-2

Slackware 14.2
x86_64
samba-4.4.16-x86_64-2

i586
samba-4.4.16-i586-2

Slackware 14.1
x86_64
samba-4.4.16-x86_64-2

96040 - Fedora Linux 26 FEDORA-2017-1f52998c8b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15923

Description

The scan detected that the host is missing the following update:
FEDORA-2017-1f52998c8b

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/2017/11/?count=200&page=1>

Fedora Core 26

konversation-1.7.4-1.fc26

96041 - Fedora Linux 27 FEDORA-2017-791c5d52be Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
FEDORA-2017-791c5d52be

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/2017/11/?count=200&page=2>

Fedora Core 27

samba-4.7.3-0.fc27

96044 - Fedora Linux 27 FEDORA-2017-72b50be8d4 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-8807

Description

The scan detected that the host is missing the following update:
FEDORA-2017-72b50be8d4

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/2017/11/?count=200&page=2>

Fedora Core 27

varnish-5.1.3-4.fc27

96046 - Fedora Linux 25 FEDORA-2017-0188f21212 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-2017-0188f21212

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/2017/11/?count=200&page=2>

Fedora Core 25

postgresql-9.5.10-1.fc25

96048 - Fedora Linux 25 FEDORA-2017-ab57a100f3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7500, CVE-2017-7501

Description

The scan detected that the host is missing the following update:
FEDORA-2017-ab57a100f3

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/2017/11/?count=200&page=1>

Fedora Core 25

rpm-4.13.0.2-1.fc25

96050 - Fedora Linux 26 FEDORA-2017-5525b6cb5a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-8807

Description

The scan detected that the host is missing the following update:
FEDORA-2017-5525b6cb5a

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/2017/11/?count=200&page=2>

Fedora Core 26

varnish-5.1.3-4.fc26

96051 - Fedora Linux 25 FEDORA-2017-f58bbbbdb0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15923

Description

The scan detected that the host is missing the following update:
FEDORA-2017-f58bbbbdb0

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/2017/11/?count=200&page=1>

Fedora Core 25

konversation-1.7.4-1.fc25

130954 - Debian Linux 8.0 DSA-4046-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-8028

Description

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

DSA-4046-1

Observation

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

<http://www.debian.org/security/2017/dsa-4046>

Debian 8.0
all
libspring-ldap-java_1.3.1.RELEASE-5+deb8u1

130956 - Debian Linux 8.0, 9.0 DSA-4047-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15864, CVE-2017-16664

Description

The scan detected that the host is missing the following update:
DSA-4047-1

Observation

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

<http://www.debian.org/security/2017/dsa-4047>

Debian 8.0
all
otrs2_3.3.18-1+deb8u2

Debian 9.0
all
otrs2_5.0.16-1+deb9u3

141783 - Red Hat Enterprise Linux RHSA-2017-3270 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-12613

Description

The scan detected that the host is missing the following update:
RHSA-2017-3270

Observation

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

<http://www.redhat.com/archives/rhsa-announce/2017-November/msg00038.html>

RHEL7S
x86_64
apr-1.4.8-3.el7_4.1

apr-debuginfo-1.4.8-3.el7_4.1
apr-devel-1.4.8-3.el7_4.1

RHEL6S

i386
apr-devel-1.3.9-5.el6_9.1
apr-debuginfo-1.3.9-5.el6_9.1
apr-1.3.9-5.el6_9.1

x86_64

apr-devel-1.3.9-5.el6_9.1
apr-debuginfo-1.3.9-5.el6_9.1
apr-1.3.9-5.el6_9.1

RHEL6WS

x86_64
apr-devel-1.3.9-5.el6_9.1
apr-debuginfo-1.3.9-5.el6_9.1
apr-1.3.9-5.el6_9.1

i386

apr-devel-1.3.9-5.el6_9.1
apr-debuginfo-1.3.9-5.el6_9.1
apr-1.3.9-5.el6_9.1

RHEL7D

x86_64
apr-1.4.8-3.el7_4.1
apr-debuginfo-1.4.8-3.el7_4.1
apr-devel-1.4.8-3.el7_4.1

RHEL6D

x86_64
apr-devel-1.3.9-5.el6_9.1
apr-debuginfo-1.3.9-5.el6_9.1
apr-1.3.9-5.el6_9.1

i386

apr-devel-1.3.9-5.el6_9.1
apr-debuginfo-1.3.9-5.el6_9.1
apr-1.3.9-5.el6_9.1

RHEL7WS

x86_64
apr-1.4.8-3.el7_4.1
apr-debuginfo-1.4.8-3.el7_4.1
apr-devel-1.4.8-3.el7_4.1

182526 - FreeBSD exim Remote Code Execution, Deny Of Service In BDAT (68b29058-d348-11e7-b9fe-c13eb7bcbf4f)

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:

exim -- remote code execution, deny of service in BDAT (68b29058-d348-11e7-b9fe-c13eb7bcbf4f)

Observation

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

<http://www.vuxml.org/freebsd/68b29058-d348-11e7-b9fe-c13eb7bcbf4f.html>

Affected packages:
4.88 <= exim < 4.89_2

182528 - FreeBSD mybb Multiple Vulnerabilities (7761288c-d148-11e7-87e5-00e04c1ea73d)

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:
mybb -- multiple vulnerabilities (7761288c-d148-11e7-87e5-00e04c1ea73d)

Observation

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

<http://www.vuxml.org/freebsd/7761288c-d148-11e7-87e5-00e04c1ea73d.html>

Affected packages:
mybb < 1.8.13

182529 - FreeBSD palemoon Multiple Vulnerabilities (6056bf68-f570-4e70-b740-b9f606971283)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Low
CVE: CVE-2017-7832, CVE-2017-7835, CVE-2017-7840

Description

The scan detected that the host is missing the following update:
palemoon -- multiple vulnerabilities (6056bf68-f570-4e70-b740-b9f606971283)

Observation

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

<http://www.vuxml.org/freebsd/6056bf68-f570-4e70-b740-b9f606971283.html>

Affected packages:
palemoon < 27.6.2

182530 - FreeBSD codeigniter Input Validation Bypass (ef3423e4-d056-11e7-a52c-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:
codeigniter -- input validation bypass (ef3423e4-d056-11e7-a52c-002590263bf5)

Observation

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

<http://www.vuxml.org/freebsd/ef3423e4-d056-11e7-a52c-002590263bf5.html>

Affected packages:
codeigniter < 3.1.6

185985 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3495-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000229

Description

The scan detected that the host is missing the following update:
USN-3495-1

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-November/004163.html>

Ubuntu 16.04

optipng_0.7.6-1ubuntu0.16.04.1

Ubuntu 14.04

optipng_0.6.4-1ubuntu0.14.04.2

Ubuntu 17.04

optipng_0.7.6-1ubuntu0.17.04.1

Ubuntu 17.10

optipng_0.7.6-1ubuntu0.17.10.1

185986 - Ubuntu Linux 17.04, 17.10 USN-3493-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-16943

Description

The scan detected that the host is missing the following update:
USN-3493-1

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-November/004161.html>

Ubuntu 17.10

exim4-daemon-light_4.89-5ubuntu1.1
exim4-daemon-heavy_4.89-5ubuntu1.1

Ubuntu 17.04

exim4-daemon-light_4.88-5ubuntu1.2
exim4-daemon-heavy_4.88-5ubuntu1.2

185993 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3477-2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-7826, CVE-2017-7827, CVE-2017-7828, CVE-2017-7830, CVE-2017-7831, CVE-2017-7832, CVE-2017-7833, CVE-2017-7834, CVE-2017-7835, CVE-2017-7837, CVE-2017-7838, CVE-2017-7839, CVE-2017-7840, CVE-2017-7842

Description

The scan detected that the host is missing the following update:
USN-3477-2

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-November/004164.html>

Ubuntu 16.04

firefox_57.0+build4-0ubuntu0.16.04.6

Ubuntu 14.04

firefox_57.0+build4-0ubuntu0.14.04.5

Ubuntu 17.04

firefox_57.0+build4-0ubuntu0.17.04.6

Ubuntu 17.10

firefox_57.0+build4-0ubuntu0.17.10.6

192986 - Fedora Linux 26 FEDORA-2017-ea72793352 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-ea72793352

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/2017/11/?count=200&page=2>

Fedora Core 26

fedpkg-1.30-4.fc26
rpkg-1.51-2.fc26

192991 - Fedora Linux 25 FEDORA-2017-f5ad4107cc 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-f5ad4107cc

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/2017/11/?count=200&page=2>

Fedora Core 25

rpkg-1.51-2.fc25
fedpkg-1.30-4.fc25

192992 - Fedora Linux 25 FEDORA-2017-8575fbfe90 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-8807

Description

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

FEDORA-2017-8575fbfe90

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/2017/11/?count=200&page=1>

Fedora Core 25

varnish-5.0.0-5.fc25

192993 - Fedora Linux 26 FEDORA-2017-1f1fdab532 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-2017-1f1fdab532

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/2017/11/?count=200&page=2>

Fedora Core 26

postgresql-9.6.6-1.fc26

192994 - Fedora Linux 26 FEDORA-2017-b52f851dea 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-b52f851dea

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/2017/11/?count=200&page=2>

Fedora Core 26

calamares-3.1.8-1.fc26

192995 - Fedora Linux 26 FEDORA-2017-59251d350d 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-2017-59251d350d

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/2017/11/?count=200&page=2>

Fedora Core 26

mediawiki-1.28.3-1.fc26

192997 - Fedora Linux 26 FEDORA-2017-366046c758 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-14746, CVE-2017-15275

Description

The scan detected that the host is missing the following update:
FEDORA-2017-366046c758

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/2017/11/?count=200&page=2>

Fedora Core 26

samba-4.6.11-0.fc26

146092 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:3106-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-13080, CVE-2017-13081

Description

The scan detected that the host is missing the following update:
SUSE-SU-2017:3106-1

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-November/003419.html>

SuSE SLES 12 SP2

noarch

kernel-firmware-20170530-21.13.1

ucode-amd-20170530-21.13.1

SuSE SLED 12 SP3

noarch

kernel-firmware-20170530-21.13.1

ucode-amd-20170530-21.13.1

SuSE SLED 12 SP2

noarch

kernel-firmware-20170530-21.13.1

ucode-amd-20170530-21.13.1

SuSE SLES 12 SP3
noarch
kernel-firmware-20170530-21.13.1
ucode-amd-20170530-21.13.1

185991 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3491-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-3209, CVE-2017-1000231, CVE-2017-1000232

Description

The scan detected that the host is missing the following update:
USN-3491-1

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-November/004159.html>

Ubuntu 16.04

libldns1_1.6.17-8ubuntu0.1

Ubuntu 14.04

libldns1_1.6.17-1ubuntu0.1

Ubuntu 17.04

libldns2_1.7.0-1ubuntu1.17.04.1

Ubuntu 17.10

libldns2_1.7.0-1ubuntu1.17.10.1

22794 - MacOS High Sierra Login As Root With No Password Vulnerability

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

An issue is present in some versions of Apple Mac OS X.

Observation

Apple macOS is the operating system developed by Apple.

An issue is present in some versions of Apple Mac OS X. The flaw is due to enabling default root user without setting password. Successful exploitation could allow an attacker to bypass security and gain admin rights without entering a password. This is observed only when default root is enabled with empty password or root is disabled. Setting password for root makes it not vulnerable.

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.

192934 - Fedora Linux 27 FEDORA-2017-5adf087854 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-7319

[Update Details](#)

Risk is updated

192968 - Fedora Linux 26 FEDORA-2017-69e06543c1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-7319

[Update Details](#)

Risk is updated

192983 - Fedora Linux 25 FEDORA-2017-c7514691cb Update Is Not Installed

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

Risk Level: High

CVE: CVE-2008-7319

[Update Details](#)

Risk is updated

22670 - Trihedral VTScada Multiple Vulnerabilities Prior To 11.3.05

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

Risk Level: High

CVE: CVE-2017-14029, CVE-2017-14031

[Update Details](#)

Risk is updated

182520 - FreeBSD cacti Multiple Vulnerabilities (db570002-ce06-11e7-804e-c85b763a2f96)

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

Risk Level: High

CVE: CVE-2017-16641, CVE-2017-16660, CVE-2017-16661, CVE-2017-16785

[Update Details](#)

Risk is updated

13718 - HP System Health Application And Command Line Utilities For Linux Unspecified Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High
CVE: CVE-2012-2000

[Update Details](#)

FASLScript is updated

878 - SSHv1 Protocol Enabled

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High
CVE: CVE-2001-0572

[Update Details](#)

FASLScript is updated

22727 - (MSPT-Nov2017) Microsoft Office Memory Handling Remote Code Execution (CVE-2017-11882)

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

Risk Level: High
CVE: CVE-2017-11882

[Update Details](#)

Recommendation is updated

130926 - Debian Linux 9.0 DSA-4023-1 Update Is Not Installed

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

Risk Level: High
CVE: CVE-2017-15566

[Update Details](#)

Risk is updated

130953 - Debian Linux 9.0 DSA-4036-1 Update Is Not Installed

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

Risk Level: High
CVE: CVE-2017-8808, CVE-2017-8809, CVE-2017-8810, CVE-2017-8811, CVE-2017-8812, CVE-2017-8814, CVE-2017-8815

[Update Details](#)

Risk is updated

192900 - Fedora Linux 27 FEDORA-2017-4dad5165dc Update Is Not Installed

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

Risk Level: High
CVE: CVE-2017-15566

[Update Details](#)

Risk is updated

22713 - (HT208224) Apple iTunes Vulnerabilities Prior To 12.7.1

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

Risk Level: Medium

CVE: CVE-2017-13783, CVE-2017-13784, CVE-2017-13785, CVE-2017-13788, CVE-2017-13791, CVE-2017-13792, CVE-2017-13793, CVE-2017-13794, CVE-2017-13795, CVE-2017-13796, CVE-2017-13797, CVE-2017-13798, CVE-2017-13802, CVE-2017-13803

[Update Details](#)

Risk is updated

22721 - (HT208225) Apple iCloud Vulnerabilities Prior To 7.1

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

Risk Level: Medium

CVE: CVE-2017-13783, CVE-2017-13784, CVE-2017-13785, CVE-2017-13788, CVE-2017-13791, CVE-2017-13792, CVE-2017-13793, CVE-2017-13794, CVE-2017-13795, CVE-2017-13796, CVE-2017-13797, CVE-2017-13798, CVE-2017-13802, CVE-2017-13803

[Update Details](#)

Risk is updated

22722 - (HT208223) Apple Safari Vulnerabilities Prior To 11.0.1

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

Risk Level: Medium

CVE: CVE-2017-13783, CVE-2017-13784, CVE-2017-13785, CVE-2017-13788, CVE-2017-13789, CVE-2017-13790, CVE-2017-13791, CVE-2017-13792, CVE-2017-13793, CVE-2017-13794, CVE-2017-13795, CVE-2017-13796, CVE-2017-13797, CVE-2017-13798, CVE-2017-13802, CVE-2017-13803

[Update Details](#)

Risk is updated

22723 - Advantech WebAccess Two Vulnerabilities Prior To 8.2.20170817

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

Risk Level: Medium

CVE: CVE-2017-12719, CVE-2017-14016

[Update Details](#)

Risk is updated

130919 - Debian Linux 8.0, 9.0 DSA-4007-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000257

[Update Details](#)

Risk is updated

146077 - SuSE Linux 42.3 openSUSE-SU-2017:3018-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15535

[Update Details](#)

Risk is updated

170900 - Amazon Linux AMI ALAS-2017-922 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000257

[Update Details](#)

Risk is updated

182498 - FreeBSD cURL Out Of Bounds Read (143ec3d6-b7cf-11e7-ac58-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2017-1000257

[Update Details](#)

Risk is updated

185938 - Ubuntu Linux 14.04, 16.04, 17.04, 17.10 USN-3457-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000257

[Update Details](#)

Risk is updated

185976 - Ubuntu Linux 16.04, 17.04, 17.10 USN-3481-1 Update Is Not Installed

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

Risk Level: Medium

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

[Update Details](#)

Risk is updated

192867 - Fedora Linux 26 FEDORA-2017-ebf32659bf Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000257

[Update Details](#)

Risk is updated

192893 - Fedora Linux 27 FEDORA-2017-b25c8a7087 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000257

[Update Details](#)

Risk is updated

192910 - Fedora Linux 27 FEDORA-2017-3433c9245d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13788, CVE-2017-13798, CVE-2017-13803

[Update Details](#)

Risk is updated

192918 - Fedora Linux 27 FEDORA-2017-512a6c5aae Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-13788, CVE-2017-13798, CVE-2017-13803, CVE-2017-3735, CVE-2017-3736

[Update Details](#)

Risk is updated CVE is updated

14340 - (VMSA-2012-0014) VMware vCenter CapacityIQ Directory Traversal Vulnerability (Unix)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2012-5051

[Update Details](#)

FASLScript is updated

192921 - Fedora Linux 26 FEDORA-2017-5cb8354008 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16248

[Update Details](#)

Risk is updated

192982 - Fedora Linux 25 FEDORA-2017-184d078d87 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16248

Update Details

Risk is updated

141084 - Red Hat Enterprise Linux RHSA-2016-0152 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7529

Update Details

Risk is updated

141092 - Red Hat Enterprise Linux RHSA-2016-0188 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7529

Update Details

Risk is updated

160043 - CentOS 6 CESA-2016-0152 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7529

Update Details

Risk is updated

160048 - CentOS 7 CESA-2016-0188 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7529

Update Details

Risk is updated

163005 - Oracle Enterprise Linux ELSA-2016-0152 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7529

[Update Details](#)

Risk is updated

163011 - Oracle Enterprise Linux ELSA-2016-0188 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7529

[Update Details](#)

Risk is updated

170638 - Amazon Linux AMI ALAS-2016-666 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7529

[Update Details](#)

Risk is updated

174901 - Scientific Linux Security ERRATA Moderate: sos on SL6.x (noarch) (1602-4182)

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

Risk Level: Medium

CVE: CVE-2015-7529

[Update Details](#)

Risk is updated

174903 - Scientific Linux Security ERRATA Moderate: sos on SL7.x (noarch) (1602-9448)

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

Risk Level: Medium

CVE: CVE-2015-7529

[Update Details](#)

Risk is updated

190135 - Fedora Linux 23 FEDORA-2015-84b1635e90 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7529

[Update Details](#)

Risk is updated

70074 - mcafee.fasl3.inc

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

Risk Level: Informational
CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

70087 - hp.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.

MCAFFEE 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.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2017 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates