2019-JAN-23
FSL version 7.6.92

MCAFEE FOUNDSTONE FSL UPDATE

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

NEW CHECKS

139102 - Oracle Solaris 11.4.4.4.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2014-10070, CVE-2014-10071, CVE-2014-10072, CVE-2016-10714, CVE-2016-9843, CVE-2017-12794, CVE-2017-14245, CVE-2017-14246, CVE-2017-14618, CVE-2017-14634, CVE-2017-17456, CVE-2017-17457, CVE-2017-17942, CVE-2017-18013, CVE-2017-18205, CVE-2017-18206, CVE-2017-18250, CVE-2017-6892, CVE-2017-8816, CVE-2018-1000810, CVE-2018-10177, CVE-2018-1071, CVE-2018-1083, CVE-2018-1100, CVE-2018-11625, CVE-2018-12599, CVE-2018-12600, CVE-2018-13139, CVE-2018-13153, CVE-2018-13419, CVE-2018-14434, CVE-2018-14435, CVE-2018-14436, CVE-2018-14437, CVE-2018-14551, CVE-2018-14618, CVE-2018-15209, CVE-2018-16323, CVE-2018-16328, CVE-2018-16412, CVE-2018-16413, CVE-2018-16640, CVE-2018-16642, CVE-2018-16643, CVE-2018-16644, CVE-2018-16645, CVE-2018-16749, CVE-2018-16750, CVE-2018-16839, CVE-2018-16840, CVE-2018-16842, CVE-2018-18023, CVE-2018-18024, CVE-2018-18025, CVE-2018-18065, CVE-2018-18544, CVE-2018-19131, CVE-2018-19132, CVE-2018-2767, CVE-2018-3058, CVE-2018-3066, CVE-2018-3081, CVE-2018-3133, CVE-2018-3143, CVE-2018-3144, CVE-2018-3155, CVE-2018-3156, CVE-2018-3161, CVE-2018-3162, CVE-2018-3171, CVE-2018-3173, CVE-2018-3174, CVE-2018-3185, CVE-2018-3187, CVE-2018-3200, CVE-2018-3247, CVE-2018-3251, CVE-2018-3276, CVE-2018-3277, CVE-2018-3278, CVE-2018-3282, CVE-2018-3283, CVE-2018-3284, CVE-2018-5784, CVE-2018-6188, CVE-2018-7536, CVE-2018-7537, CVE-2018-7548, CVE-2018-7549, CVE-2018-9135

Description

The scan detected that the host is missing the following update:
SRU 11.4.4.4.0

Observation

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

https://support.oracle.com/rs?type=doc&id=2483313.1
https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=507462766511768&id=1448883.1&_afrWindowMode=0&_adf.ctrl-state=98kg3qcn0_33#aref_section26

147559 - SuSE Linux 15.0 openSUSE-SU-2019:0053-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15126, CVE-2018-15127, CVE-2018-20019, CVE-2018-20020, CVE-2018-20021, CVE-2018-20022, CVE-2018-20023, CVE-2018-20024, CVE-2018-6307

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0053-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00055.html

SuSE Linux 15.0
x86_64
LibVNCServer-devel-0.9.10-lp150.3.3.1
LibVNCServer-debugsource-0.9.10-lp150.3.3.1
libvncserver0-debuginfo-0.9.10-lp150.3.3.1
libvncserver0-0.9.10-lp150.3.3.1
libvncclient0-0.9.10-lp150.3.3.1
libvncclient0-debuginfo-0.9.10-lp150.3.3.1

i586
LibVNCServer-devel-0.9.10-lp150.3.3.1
LibVNCServer-debugsource-0.9.10-lp150.3.3.1
libvncserver0-debuginfo-0.9.10-lp150.3.3.1
libvncserver0-0.9.10-lp150.3.3.1
libvncclient0-0.9.10-lp150.3.3.1
libvncclient0-debuginfo-0.9.10-lp150.3.3.1

194687 - Fedora Linux 28 FEDORA-2019-509c133845 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10322, CVE-2018-10323, CVE-2018-10840, CVE-2018-10853, CVE-2018-1108, CVE-2018-1120, CVE-2018-11506, CVE-2018-12232, CVE-2018-12633, CVE-2018-12714, CVE-2018-12896, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-13405, CVE-2018-14633, CVE-2018-14678, CVE-2018-14734, CVE-2018-15471, CVE-2018-16862, CVE-2018-17182, CVE-2018-18710, CVE-2018-19406, CVE-2018-19407, CVE-2018-19824, CVE-2018-3620, CVE-2018-3639, CVE-2018-3646, CVE-2018-5391, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701

Description

The scan detected that the host is missing the following update:
FEDORA-2019-509c133845

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/2019/1/?count=200&page=2

Fedora Core 28

kernel-4.19.15-200.fc28
kernel-headers-4.19.15-200.fc28

194709 - Fedora Linux 28 FEDORA-2019-20a89ca9af Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10322, CVE-2018-10323, CVE-2018-10840, CVE-2018-10853, CVE-2018-1108, CVE-2018-1120, CVE-2018-11506, CVE-2018-12232, CVE-2018-12633, CVE-2018-12714, CVE-2018-12896, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-13405, CVE-2018-14633, CVE-2018-14678, CVE-2018-14734, CVE-2018-15471, CVE-2018-16862, CVE-2018-16884, CVE-2018-17182, CVE-2018-18710, CVE-2018-19406, CVE-2018-19407, CVE-2018-19824, CVE-2018-3620, CVE-2018-3639, CVE-2018-3646, CVE-2018-5391, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701

Description

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

FEDORA-2019-20a89ca9af

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/2019/1/?count=200&page=1

Fedora Core 28

kernel-4.19.16-200.fc28
kernel-headers-4.19.16-200.fc28
kernel-tools-4.19.16-200.fc28

24631 - Advantech WebAccess Improper Input Validation Vulnerability (ICSA-18-352-02)

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

Risk Level: High

CVE: CVE-2018-18999

Description

A vulnerability is present in some versions of Advantech WebAccess.

Observation

Advantech WebAccess is a web-based HMI software application used in energy, manufacturing, and building automation systems.

A vulnerability is present in some versions of Advantech WebAccess. The flaw is due to lack of proper validation. Successful exploitation could allow a remote attacker to execute arbitrary code on the target system.

24640 - (APSB19-05) Vulnerability In Adobe Connect

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

Risk Level: High

CVE: CVE-2018-19718

Description

A vulnerability is present in some versions of Adobe Connect.

Observation

Adobe Connect is a network meeting solution.

A vulnerability is present in some versions of Adobe Connect. The flaw lies in session token component. Successful exploitation could allow an attacker to cause disclosure of information.

24643 - (SYMSA1456) Symantec Management Agent Inventory Plugin Privilege Escalation Vulnerability

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

Risk Level: High

CVE: CVE-2018-5240

Description

A vulnerability is present in some versions of the Symantec ITMS.

Observation

Symantec ITMS is a network-based computer management solution.

A vulnerability is present in some versions of the Symantec ITMS. The flaw lies in the Symantec management agent component. Successful exploitation by an attacker could allow to gain elevated access to resources on the target.

24645 - (JSA10914) Juniper Junos OS QFX and PTX Series FPC Process Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2019-0014

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is an operating system used in Juniper device.

A vulnerability is present in some versions of Juniper Junos. The flaw lies in FPC process. Successful exploitation could allow an attacker to cause denial of service condition on the target system.

139104 - Oracle Solaris 11.4.5.3.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2016-8705, CVE-2017-1000456, CVE-2017-14517, CVE-2017-14518, CVE-2017-14519, CVE-2017-14520, CVE-2017-14927, CVE-2017-14975, CVE-2017-14976, CVE-2017-14977, CVE-2017-15565, CVE-2017-18267, CVE-2017-9951, CVE-2018-0734, CVE-2018-0735, CVE-2018-0739, CVE-2018-1000115, CVE-2018-1000127, CVE-2018-11763, CVE-2018-13988, CVE-2018-15909, CVE-2018-17183, CVE-2018-17961, CVE-2018-18073, CVE-2018-18284, CVE-2018-19158, CVE-2018-19518, CVE-2018-19622, CVE-2018-19623, CVE-2018-19624, CVE-2018-19625, CVE-2018-19626, CVE-2018-19627, CVE-2018-19628, CVE-2018-2767, CVE-2018-3058, CVE-2018-3062, CVE-2018-3063, CVE-2018-3064, CVE-2018-3066, CVE-2018-3070, CVE-2018-3081, CVE-2018-3133, CVE-2018-3143, CVE-2018-3156, CVE-2018-3174, CVE-2018-3247, CVE-2018-3251, CVE-2018-3276, CVE-2018-3278, CVE-2018-3282, CVE-2018-5407, CVE-2018-6797, CVE-2018-6798, CVE-2018-6913, CVE-2018-9918

Description

The scan detected that the host is missing the following update:
SRU 11.4.5.3.0

Observation

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

https://support.oracle.com/rs?type=doc&id=2492782.1
https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=507462766511768&id=1448883.1&_afrWindowMode=0&_adf.ctrl-state=98kg3qcn0_33#aref_section26

139105 - Oracle Solaris 11.4.3.5.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2015-3152, CVE-2016-6489, CVE-2016-9840, CVE-2016-9841, CVE-2016-9842, CVE-2016-9843, CVE-2017-10789, CVE-2017-17433, CVE-2017-17434, CVE-2017-6888, CVE-2018-1000161, CVE-2018-11439, CVE-2018-11646, CVE-2018-11712,

CVE-2018-11713, CVE-2018-11784, CVE-2018-12086, CVE-2018-12293, CVE-2018-12294, CVE-2018-12911, CVE-2018-14036, CVE-2018-14598, CVE-2018-14599, CVE-2018-14600, CVE-2018-14665, CVE-2018-15173, CVE-2018-17082, CVE-2018-17456, CVE-2018-18225, CVE-2018-18226, CVE-2018-18227, CVE-2018-3639, CVE-2018-3646, CVE-2018-4101, CVE-2018-4113, CVE-2018-4114, CVE-2018-4117, CVE-2018-4118, CVE-2018-4119, CVE-2018-4120, CVE-2018-4121, CVE-2018-4122, CVE-2018-4125, CVE-2018-4127, CVE-2018-4128, CVE-2018-4129, CVE-2018-4133, CVE-2018-4146, CVE-2018-4161, CVE-2018-4162, CVE-2018-4163, CVE-2018-4165, CVE-2018-4190, CVE-2018-4192, CVE-2018-4199, CVE-2018-4200, CVE-2018-4201, CVE-2018-4204, CVE-2018-4214, CVE-2018-4218, CVE-2018-4222, CVE-2018-4232, CVE-2018-4233, CVE-2018-4246, CVE-2018-4261, CVE-2018-4262, CVE-2018-4263, CVE-2018-4264, CVE-2018-4265, CVE-2018-4266, CVE-2018-4267, CVE-2018-4270, CVE-2018-4271, CVE-2018-4272, CVE-2018-4273, CVE-2018-4278, CVE-2018-4284, CVE-2018-5740, CVE-2018-5764, CVE-2019-2437

Description

The scan detected that the host is missing the following update:
SRU 11.4.3.5.0

Observation

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

https://support.oracle.com/rs?type=doc&id=2472200.1
https://support.oracle.com/epmos/faces/DocumentDisplay?_afrLoop=507462766511768&id=1448883.1&_afrWindowMode=0&_adf.ctrl-state=98kg3qcn0_33#aref_section26

147548 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:0054-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20683

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0054-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00062.html

SuSE Linux 15.0
noarch
gitolite-3.6.11-lp150.2.6.1

SuSE Linux 42.3
noarch
gitolite-3.6.11-4.6.1

147549 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0132-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20685, CVE-2019-6109, CVE-2019-6110, CVE-2019-6111

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0132-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005051.html

SuSE SLED 12 SP3
x86_64
openssh-askpass-gnome-debuginfo-7.2p2-74.35.1
openssh-debuginfo-7.2p2-74.35.1
openssh-7.2p2-74.35.1
openssh-debugsource-7.2p2-74.35.1
openssh-helpers-debuginfo-7.2p2-74.35.1
openssh-helpers-7.2p2-74.35.1
openssh-askpass-gnome-7.2p2-74.35.1

SuSE SLED 12 SP4
x86_64
openssh-askpass-gnome-debuginfo-7.2p2-74.35.1
openssh-debuginfo-7.2p2-74.35.1
openssh-7.2p2-74.35.1
openssh-debugsource-7.2p2-74.35.1
openssh-helpers-debuginfo-7.2p2-74.35.1
openssh-helpers-7.2p2-74.35.1
openssh-askpass-gnome-7.2p2-74.35.1

SuSE SLES 12 SP4
x86_64
openssh-askpass-gnome-debuginfo-7.2p2-74.35.1
openssh-debuginfo-7.2p2-74.35.1
openssh-7.2p2-74.35.1
openssh-debugsource-7.2p2-74.35.1
openssh-helpers-debuginfo-7.2p2-74.35.1
openssh-helpers-7.2p2-74.35.1
openssh-fips-7.2p2-74.35.1
openssh-askpass-gnome-7.2p2-74.35.1

SuSE SLES 12 SP3
x86_64
openssh-askpass-gnome-debuginfo-7.2p2-74.35.1
openssh-debuginfo-7.2p2-74.35.1
openssh-7.2p2-74.35.1
openssh-debugsource-7.2p2-74.35.1
openssh-helpers-debuginfo-7.2p2-74.35.1
openssh-helpers-7.2p2-74.35.1
openssh-fips-7.2p2-74.35.1
openssh-askpass-gnome-7.2p2-74.35.1

147551 - SuSE Linux 42.3 openSUSE-SU-2019:0064-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6250

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0064-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00063.html

SuSE Linux 42.3
x86_64
libzmq5-debuginfo-32bit-4.2.2-2.8.1
zeromq-debugsource-4.2.2-2.8.1
libzmq5-debuginfo-4.2.2-2.8.1
libzmq5-32bit-4.2.2-2.8.1
libzmq5-4.2.2-2.8.1
zeromq-devel-4.2.2-2.8.1
zeromq-tools-debuginfo-4.2.2-2.8.1
zeromq-tools-4.2.2-2.8.1

i586
zeromq-debugsource-4.2.2-2.8.1
libzmq5-debuginfo-4.2.2-2.8.1
libzmq5-4.2.2-2.8.1
zeromq-devel-4.2.2-2.8.1
zeromq-tools-debuginfo-4.2.2-2.8.1
zeromq-tools-4.2.2-2.8.1

147552 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0119-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9843, CVE-2018-3143, CVE-2018-3156, CVE-2018-3162, CVE-2018-3173, CVE-2018-3174, CVE-2018-3185, CVE-2018-3200, CVE-2018-3251, CVE-2018-3277, CVE-2018-3282, CVE-2018-3284

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0119-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005041.html

SuSE SLED 12 SP4
x86_64
mariadb-debugsource-10.2.21-3.7.1
mariadb-10.2.21-3.7.1
mariadb-client-10.2.21-3.7.1
mariadb-client-debuginfo-10.2.21-3.7.1
mariadb-debuginfo-10.2.21-3.7.1

noarch
mariadb-errormessages-10.2.21-3.7.1

SuSE SLES 12 SP4
noarch
mariadb-errormessages-10.2.21-3.7.1

x86_64

mariadb-debugsource-10.2.21-3.7.1
mariadb-client-10.2.21-3.7.1
mariadb-10.2.21-3.7.1
mariadb-tools-10.2.21-3.7.1
mariadb-tools-debuginfo-10.2.21-3.7.1
mariadb-client-debuginfo-10.2.21-3.7.1
mariadb-debuginfo-10.2.21-3.7.1

147553 - SuSE Linux 42.3 openSUSE-SU-2019:0052-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9116, CVE-2018-14349, CVE-2018-14350, CVE-2018-14351, CVE-2018-14352, CVE-2018-14353, CVE-2018-14354, CVE-2018-14355, CVE-2018-14356, CVE-2018-14357, CVE-2018-14358, CVE-2018-14359, CVE-2018-14360, CVE-2018-14361, CVE-2018-14362, CVE-2018-14363

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0052-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00052.html

SuSE Linux 42.3
x86_64
mutt-debugsource-1.10.1-2.5.1
mutt-debuginfo-1.10.1-2.5.1
mutt-1.10.1-2.5.1

noarch
mutt-doc-1.10.1-2.5.1
mutt-lang-1.10.1-2.5.1

147554 - SuSE SLED 12 SP3, 12 SP4 SUSE-SU-2019:0134-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-0886, CVE-2018-1000852, CVE-2018-8784, CVE-2018-8785, CVE-2018-8786, CVE-2018-8787, CVE-2018-8788, CVE-2018-8789

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0134-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005053.html

SuSE SLED 12 SP4
x86_64
freerdp-2.0.0~git.1463131968.4e66df7-12.8.1

freerdp-debugsource-2.0.0~git.1463131968.4e66df7-12.8.1
freerdp-debuginfo-2.0.0~git.1463131968.4e66df7-12.8.1
libfreerdp2-2.0.0~git.1463131968.4e66df7-12.8.1
libfreerdp2-debuginfo-2.0.0~git.1463131968.4e66df7-12.8.1

SuSE SLED 12 SP3
x86_64
freerdp-2.0.0~git.1463131968.4e66df7-12.8.1
freerdp-debugsource-2.0.0~git.1463131968.4e66df7-12.8.1
freerdp-debuginfo-2.0.0~git.1463131968.4e66df7-12.8.1
libfreerdp2-2.0.0~git.1463131968.4e66df7-12.8.1
libfreerdp2-debuginfo-2.0.0~git.1463131968.4e66df7-12.8.1

147555 - SuSE SLES 11 SP4 SUSE-SU-2019:13931-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20685, CVE-2019-6109, CVE-2019-6110, CVE-2019-6111

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13931-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005049.html

SuSE SLES 11 SP4
i586
openssh-fips-6.6p1-36.12.1
openssh-helpers-6.6p1-36.12.1
openssh-askpass-gnome-6.6p1-36.12.1
openssh-6.6p1-36.12.1

x86_64
openssh-fips-6.6p1-36.12.1
openssh-helpers-6.6p1-36.12.1
openssh-askpass-gnome-6.6p1-36.12.1
openssh-6.6p1-36.12.1

147556 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0135-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16864, CVE-2018-16865, CVE-2018-16866

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0135-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005052.html

SuSE SLED 12 SP3
x86_64
libsystemd0-228-150.58.1
libudev1-32bit-228-150.58.1
libsystemd0-debuginfo-32bit-228-150.58.1
libsystemd0-32bit-228-150.58.1
udev-debuginfo-228-150.58.1
libudev1-228-150.58.1
systemd-sysvinit-228-150.58.1
libudev1-debuginfo-32bit-228-150.58.1
systemd-228-150.58.1
udev-228-150.58.1
systemd-debuginfo-228-150.58.1
systemd-debuginfo-32bit-228-150.58.1
systemd-debugsource-228-150.58.1
libudev1-debuginfo-228-150.58.1
systemd-32bit-228-150.58.1
libsystemd0-debuginfo-228-150.58.1

noarch
systemd-bash-completion-228-150.58.1

SuSE SLED 12 SP4
x86_64
libsystemd0-228-150.58.1
libudev1-32bit-228-150.58.1
libsystemd0-debuginfo-32bit-228-150.58.1
libsystemd0-32bit-228-150.58.1
udev-debuginfo-228-150.58.1
libudev1-228-150.58.1
systemd-sysvinit-228-150.58.1
libudev1-debuginfo-32bit-228-150.58.1
systemd-228-150.58.1
udev-228-150.58.1
systemd-debuginfo-228-150.58.1
systemd-debuginfo-32bit-228-150.58.1
systemd-debugsource-228-150.58.1
libudev1-debuginfo-228-150.58.1
systemd-32bit-228-150.58.1
libsystemd0-debuginfo-228-150.58.1

noarch
systemd-bash-completion-228-150.58.1

SuSE SLES 12 SP4
noarch
systemd-bash-completion-228-150.58.1

x86_64
libsystemd0-228-150.58.1
libudev1-32bit-228-150.58.1
libsystemd0-debuginfo-32bit-228-150.58.1
libsystemd0-32bit-228-150.58.1
libudev1-228-150.58.1
systemd-sysvinit-228-150.58.1
libudev1-debuginfo-32bit-228-150.58.1
systemd-228-150.58.1
udev-228-150.58.1

systemd-debuginfo-228-150.58.1
udev-debuginfo-228-150.58.1
systemd-debugsource-228-150.58.1
libudev1-debuginfo-228-150.58.1
systemd-32bit-228-150.58.1
systemd-debuginfo-32bit-228-150.58.1
libsystemd0-debuginfo-228-150.58.1

SuSE SLES 12 SP3
noarch
systemd-bash-completion-228-150.58.1

x86_64
libsystemd0-228-150.58.1
libudev1-32bit-228-150.58.1
libsystemd0-debuginfo-32bit-228-150.58.1
libsystemd0-32bit-228-150.58.1
libudev1-228-150.58.1
systemd-sysvinit-228-150.58.1
libudev1-debuginfo-32bit-228-150.58.1
systemd-228-150.58.1
udev-228-150.58.1
systemd-debuginfo-228-150.58.1
udev-debuginfo-228-150.58.1
systemd-debugsource-228-150.58.1
libudev1-debuginfo-228-150.58.1
systemd-32bit-228-150.58.1
systemd-debuginfo-32bit-228-150.58.1
libsystemd0-debuginfo-228-150.58.1

147560 - SuSE Linux 15.0, 42.3 openSUSE-SU-2019:0058-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-4013, CVE-2019-6256

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0058-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00064.html

SuSE Linux 15.0
x86_64
live555-devel-2018.12.14-lp150.2.3.1

SuSE Linux 42.3
x86_64
live555-devel-2018.12.14-7.3.1

i586
live555-devel-2018.12.14-7.3.1

147563 - SuSE Linux 15.0 openSUSE-SU-2019:0065-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-12232, CVE-2018-14625, CVE-2018-16862, CVE-2018-16884, CVE-2018-18397, CVE-2018-19407, CVE-2018-19824, CVE-2018-19854, CVE-2018-19985, CVE-2018-20169, CVE-2018-9568

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0065-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00059.html

SuSE Linux 15.0
x86_64
kernel-debug-devel-debuginfo-4.12.14-lp150.12.45.1
kernel-syms-4.12.14-lp150.12.45.1
kernel-vanilla-debuginfo-4.12.14-lp150.12.45.1
kernel-obs-build-debugsource-4.12.14-lp150.12.45.1
kernel-default-devel-4.12.14-lp150.12.45.1
kernel-vanilla-base-debuginfo-4.12.14-lp150.12.45.1
kernel-debug-devel-4.12.14-lp150.12.45.1
kernel-vanilla-devel-4.12.14-lp150.12.45.1
kernel-obs-build-4.12.14-lp150.12.45.1
kernel-kvmsmall-devel-4.12.14-lp150.12.45.1
kernel-default-debugsource-4.12.14-lp150.12.45.1
kernel-debug-4.12.14-lp150.12.45.1
kernel-debug-debugsource-4.12.14-lp150.12.45.1
kernel-kvmsmall-debuginfo-4.12.14-lp150.12.45.1
kernel-default-base-4.12.14-lp150.12.45.1
kernel-kvmsmall-4.12.14-lp150.12.45.1
kernel-debug-base-4.12.14-lp150.12.45.1
kernel-vanilla-base-4.12.14-lp150.12.45.1
kernel-kvmsmall-debugsource-4.12.14-lp150.12.45.1
kernel-kvmsmall-base-4.12.14-lp150.12.45.1
kernel-debug-base-debuginfo-4.12.14-lp150.12.45.1
kernel-vanilla-4.12.14-lp150.12.45.1
kernel-debug-debuginfo-4.12.14-lp150.12.45.1
kernel-default-devel-debuginfo-4.12.14-lp150.12.45.1
kernel-kvmsmall-base-debuginfo-4.12.14-lp150.12.45.1
kernel-default-debuginfo-4.12.14-lp150.12.45.1
kernel-obs-qa-4.12.14-lp150.12.45.1
kernel-vanilla-debugsource-4.12.14-lp150.12.45.1
kernel-kvmsmall-devel-debuginfo-4.12.14-lp150.12.45.1
kernel-default-base-debuginfo-4.12.14-lp150.12.45.1
kernel-vanilla-devel-debuginfo-4.12.14-lp150.12.45.1
kernel-default-4.12.14-lp150.12.45.1

noarch
kernel-macros-4.12.14-lp150.12.45.1
kernel-source-4.12.14-lp150.12.45.1
kernel-devel-4.12.14-lp150.12.45.1
kernel-docs-4.12.14-lp150.12.45.1
kernel-docs-html-4.12.14-lp150.12.45.1
kernel-source-vanilla-4.12.14-lp150.12.45.1

147564 - SuSE Linux 15.0 openSUSE-SU-2019:0057-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20483

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0057-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00054.html

SuSE Linux 15.0
x86_64
wget-1.19.5-lp150.2.3.1
wget-debugsource-1.19.5-lp150.2.3.1
wget-debuginfo-1.19.5-lp150.2.3.1

i586
wget-1.19.5-lp150.2.3.1
wget-debugsource-1.19.5-lp150.2.3.1
wget-debuginfo-1.19.5-lp150.2.3.1

147565 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0128-1 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-2019:0128-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005047.html

SuSE SLES 12 SP3
noarch
PackageKit-lang-1.1.3-24.9.1

x86_64
libpackagekit-glib2-18-1.1.3-24.9.1
PackageKit-debugsource-1.1.3-24.9.1
libpackagekit-glib2-18-debuginfo-1.1.3-24.9.1
PackageKit-debuginfo-1.1.3-24.9.1
PackageKit-backend-zypp-debuginfo-1.1.3-24.9.1
PackageKit-backend-zypp-1.1.3-24.9.1
PackageKit-1.1.3-24.9.1

typelib-1_0-PackageKitGlib-1_0-1.1.3-24.9.1

SuSE SLES 12 SP4
noarch
PackageKit-lang-1.1.3-24.9.1

x86_64
libpackagekit-glib2-18-1.1.3-24.9.1
PackageKit-debugsource-1.1.3-24.9.1
libpackagekit-glib2-18-debuginfo-1.1.3-24.9.1
PackageKit-debuginfo-1.1.3-24.9.1
PackageKit-backend-zypp-debuginfo-1.1.3-24.9.1
PackageKit-backend-zypp-1.1.3-24.9.1
PackageKit-1.1.3-24.9.1
typelib-1_0-PackageKitGlib-1_0-1.1.3-24.9.1

SuSE SLED 12 SP4
x86_64
libpackagekit-glib2-18-1.1.3-24.9.1
PackageKit-1.1.3-24.9.1
PackageKit-gtk3-module-1.1.3-24.9.1
typelib-1_0-PackageKitGlib-1_0-1.1.3-24.9.1
libpackagekit-glib2-18-debuginfo-1.1.3-24.9.1
PackageKit-debuginfo-1.1.3-24.9.1
PackageKit-debugsource-1.1.3-24.9.1
PackageKit-gstreamer-plugin-1.1.3-24.9.1
PackageKit-backend-zypp-debuginfo-1.1.3-24.9.1
PackageKit-gstreamer-plugin-debuginfo-1.1.3-24.9.1
PackageKit-gtk3-module-debuginfo-1.1.3-24.9.1
PackageKit-backend-zypp-1.1.3-24.9.1

noarch
PackageKit-lang-1.1.3-24.9.1

SuSE SLED 12 SP3
x86_64
libpackagekit-glib2-18-1.1.3-24.9.1
PackageKit-1.1.3-24.9.1
PackageKit-gtk3-module-1.1.3-24.9.1
typelib-1_0-PackageKitGlib-1_0-1.1.3-24.9.1
libpackagekit-glib2-18-debuginfo-1.1.3-24.9.1
PackageKit-debuginfo-1.1.3-24.9.1
PackageKit-debugsource-1.1.3-24.9.1
PackageKit-gstreamer-plugin-1.1.3-24.9.1
PackageKit-backend-zypp-debuginfo-1.1.3-24.9.1
PackageKit-gstreamer-plugin-debuginfo-1.1.3-24.9.1
PackageKit-gtk3-module-debuginfo-1.1.3-24.9.1
PackageKit-backend-zypp-1.1.3-24.9.1

noarch
PackageKit-lang-1.1.3-24.9.1

147566 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0111-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20217

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0111-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005038.html

SuSE SLED 12 SP3
x86_64
krb5-debuginfo-1.12.5-40.31.1
krb5-1.12.5-40.31.1
krb5-client-1.12.5-40.31.1
krb5-debuginfo-32bit-1.12.5-40.31.1
krb5-debugsource-1.12.5-40.31.1
krb5-32bit-1.12.5-40.31.1
krb5-client-debuginfo-1.12.5-40.31.1

SuSE SLED 12 SP4
x86_64
krb5-debuginfo-1.12.5-40.31.1
krb5-1.12.5-40.31.1
krb5-client-1.12.5-40.31.1
krb5-debuginfo-32bit-1.12.5-40.31.1
krb5-debugsource-1.12.5-40.31.1
krb5-32bit-1.12.5-40.31.1
krb5-client-debuginfo-1.12.5-40.31.1

SuSE SLES 12 SP4
x86_64
krb5-client-1.12.5-40.31.1
krb5-plugin-preauth-pkinit-1.12.5-40.31.1
krb5-plugin-preauth-otp-1.12.5-40.31.1
krb5-1.12.5-40.31.1
krb5-doc-1.12.5-40.31.1
krb5-debuginfo-32bit-1.12.5-40.31.1
krb5-debugsource-1.12.5-40.31.1
krb5-32bit-1.12.5-40.31.1
krb5-plugin-kdb-ldap-1.12.5-40.31.1
krb5-client-debuginfo-1.12.5-40.31.1
krb5-plugin-kdb-ldap-debuginfo-1.12.5-40.31.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.5-40.31.1
krb5-debuginfo-1.12.5-40.31.1
krb5-server-1.12.5-40.31.1
krb5-plugin-preauth-otp-debuginfo-1.12.5-40.31.1
krb5-server-debuginfo-1.12.5-40.31.1

SuSE SLES 12 SP3
x86_64
krb5-client-1.12.5-40.31.1
krb5-plugin-preauth-pkinit-1.12.5-40.31.1
krb5-plugin-preauth-otp-1.12.5-40.31.1
krb5-1.12.5-40.31.1
krb5-doc-1.12.5-40.31.1
krb5-debuginfo-32bit-1.12.5-40.31.1
krb5-debugsource-1.12.5-40.31.1
krb5-32bit-1.12.5-40.31.1
krb5-plugin-kdb-ldap-1.12.5-40.31.1
krb5-client-debuginfo-1.12.5-40.31.1

krb5-plugin-kdb-ldap-debuginfo-1.12.5-40.31.1
krb5-plugin-preauth-pkinit-debuginfo-1.12.5-40.31.1
krb5-debuginfo-1.12.5-40.31.1
krb5-server-1.12.5-40.31.1
krb5-plugin-preauth-otp-debuginfo-1.12.5-40.31.1
krb5-server-debuginfo-1.12.5-40.31.1

147567 - SuSE Linux 15.0 openSUSE-SU-2019:0063-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20217

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0063-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00053.html

SuSE Linux 15.0
x86_64
krb5-server-debuginfo-1.15.2-lp150.5.3.1
krb5-32bit-debuginfo-1.15.2-lp150.5.3.1
krb5-debugsource-1.15.2-lp150.5.3.1
krb5-mini-debuginfo-1.15.2-lp150.5.3.1
krb5-plugin-preauth-pkinit-1.15.2-lp150.5.3.1
krb5-32bit-1.15.2-lp150.5.3.1
krb5-devel-32bit-1.15.2-lp150.5.3.1
krb5-plugin-preauth-otp-1.15.2-lp150.5.3.1
krb5-server-1.15.2-lp150.5.3.1
krb5-1.15.2-lp150.5.3.1
krb5-mini-debugsource-1.15.2-lp150.5.3.1
krb5-plugin-kdb-ldap-1.15.2-lp150.5.3.1
krb5-plugin-kdb-ldap-debuginfo-1.15.2-lp150.5.3.1
krb5-devel-1.15.2-lp150.5.3.1
krb5-client-debuginfo-1.15.2-lp150.5.3.1
krb5-plugin-preauth-otp-debuginfo-1.15.2-lp150.5.3.1
krb5-client-1.15.2-lp150.5.3.1
krb5-plugin-preauth-pkinit-debuginfo-1.15.2-lp150.5.3.1
krb5-debuginfo-1.15.2-lp150.5.3.1
krb5-mini-1.15.2-lp150.5.3.1
krb5-mini-devel-1.15.2-lp150.5.3.1

i586
krb5-server-debuginfo-1.15.2-lp150.5.3.1
krb5-debugsource-1.15.2-lp150.5.3.1
krb5-mini-debuginfo-1.15.2-lp150.5.3.1
krb5-plugin-preauth-pkinit-1.15.2-lp150.5.3.1
krb5-plugin-preauth-otp-1.15.2-lp150.5.3.1
krb5-server-1.15.2-lp150.5.3.1
krb5-1.15.2-lp150.5.3.1
krb5-mini-debugsource-1.15.2-lp150.5.3.1
krb5-plugin-kdb-ldap-1.15.2-lp150.5.3.1
krb5-plugin-kdb-ldap-debuginfo-1.15.2-lp150.5.3.1

krb5-devel-1.15.2-lp150.5.3.1
krb5-client-debuginfo-1.15.2-lp150.5.3.1
krb5-plugin-preauth-otp-debuginfo-1.15.2-lp150.5.3.1
krb5-client-1.15.2-lp150.5.3.1
krb5-plugin-preauth-pkinit-debuginfo-1.15.2-lp150.5.3.1
krb5-debuginfo-1.15.2-lp150.5.3.1
krb5-mini-1.15.2-lp150.5.3.1
krb5-mini-devel-1.15.2-lp150.5.3.1

160504 - CentOS 7 CESA-2019-0059 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15127

Description

The scan detected that the host is missing the following update:
CESA-2019-0059

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-January/023144.html

CentOS 7
x86_64
libvncserver-devel-0.9.9-13.el7_6
libvncserver-0.9.9-13.el7_6

i686
libvncserver-devel-0.9.9-13.el7_6
libvncserver-0.9.9-13.el7_6

163788 - Oracle Enterprise Linux ELSA-2019-0109 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18311

Description

The scan detected that the host is missing the following update:
ELSA-2019-0109

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-January/008382.html

OEL7
x86_64
perl-Pod-Escapes-1.04-294.el7_6
perl-Object-Accessor-0.42-294.el7_6
perl-IO-Zlib-1.10-294.el7_6
perl-ExtUtils-Embed-1.30-294.el7_6

perl-ExtUtils-CBuilder-0.28.2.6-294.el7_6
perl-macros-5.16.3-294.el7_6
perl-Package-Constants-0.02-294.el7_6
perl-Module-Loaded-0.08-294.el7_6
perl-CPAN-1.9800-294.el7_6
perl-Module-CoreList-2.76.02-294.el7_6
perl-libs-5.16.3-294.el7_6
perl-tests-5.16.3-294.el7_6
perl-devel-5.16.3-294.el7_6
perl-core-5.16.3-294.el7_6
perl-ExtUtils-Install-1.58-294.el7_6
perl-Time-Piece-1.20.1-294.el7_6
perl-Locale-Maketext-Simple-0.21-294.el7_6
perl-5.16.3-294.el7_6

194681 - Fedora Linux 29 FEDORA-2019-026d5ab23d Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7686, CVE-2018-12558

Description

The scan detected that the host is missing the following update:
FEDORA-2019-026d5ab23d

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/2019/1/?count=200&page=2

Fedora Core 29

perl-Email-Address-1.912-1.fc29

194689 - Fedora Linux 28 FEDORA-2019-8deebad756 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-7686, CVE-2018-12558

Description

The scan detected that the host is missing the following update:
FEDORA-2019-8deebad756

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/2019/1/?count=200&page=2

Fedora Core 28

perl-Email-Address-1.912-1.fc28

194703 - Fedora Linux 29 FEDORA-2019-a171d0d192 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5882

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a171d0d192

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/2019/1/?count=200&page=1

Fedora Core 29

irssi-1.1.2-1.fc29

194708 - Fedora Linux 29 FEDORA-2019-2e385f97e2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-11333, CVE-2017-11735, CVE-2017-14160, CVE-2017-14632, CVE-2017-14633, CVE-2018-10392, CVE-2018-10393, CVE-2018-5146

Description

The scan detected that the host is missing the following update:
FEDORA-2019-2e385f97e2

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/2019/1/?count=200&page=1

Fedora Core 29

mingw-libvorbis-1.3.6-2.fc29

194710 - Fedora Linux 28 FEDORA-2019-920924ed23 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5882

Description

The scan detected that the host is missing the following update:
FEDORA-2019-920924ed23

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/2019/1/?count=200&page=1

Fedora Core 28

irssi-1.1.2-1.fc28

196234 - Red Hat Enterprise Linux RHSA-2019-0109 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18311

Description

The scan detected that the host is missing the following update:
RHSA-2019-0109

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-January/msg00018.html

RHEL7D
x86_64
perl-5.16.3-294.el7_6
perl-Time-Piece-1.20.1-294.el7_6
perl-devel-5.16.3-294.el7_6
perl-debuginfo-5.16.3-294.el7_6
perl-core-5.16.3-294.el7_6
perl-macros-5.16.3-294.el7_6
perl-libs-5.16.3-294.el7_6
perl-tests-5.16.3-294.el7_6

noarch
perl-ExtUtils-Embed-1.30-294.el7_6
perl-Module-CoreList-2.76.02-294.el7_6
perl-Object-Accessor-0.42-294.el7_6
perl-ExtUtils-Install-1.58-294.el7_6
perl-Package-Constants-0.02-294.el7_6
perl-Module-Loaded-0.08-294.el7_6
perl-CPAN-1.9800-294.el7_6
perl-IO-Zlib-1.10-294.el7_6
perl-Locale-Maketext-Simple-0.21-294.el7_6
perl-ExtUtils-CBuilder-0.28.2.6-294.el7_6
perl-Pod-Escapes-1.04-294.el7_6

RHEL7S
noarch
perl-ExtUtils-Embed-1.30-294.el7_6
perl-Module-CoreList-2.76.02-294.el7_6
perl-Object-Accessor-0.42-294.el7_6
perl-ExtUtils-Install-1.58-294.el7_6
perl-Package-Constants-0.02-294.el7_6
perl-Module-Loaded-0.08-294.el7_6
perl-CPAN-1.9800-294.el7_6
perl-IO-Zlib-1.10-294.el7_6
perl-Locale-Maketext-Simple-0.21-294.el7_6
perl-ExtUtils-CBuilder-0.28.2.6-294.el7_6

perl-Pod-Escapes-1.04-294.el7_6

x86_64
perl-5.16.3-294.el7_6
perl-Time-Piece-1.20.1-294.el7_6
perl-devel-5.16.3-294.el7_6
perl-debuginfo-5.16.3-294.el7_6
perl-core-5.16.3-294.el7_6
perl-macros-5.16.3-294.el7_6
perl-libs-5.16.3-294.el7_6
perl-tests-5.16.3-294.el7_6

RHEL7WS
x86_64
perl-5.16.3-294.el7_6
perl-Time-Piece-1.20.1-294.el7_6
perl-devel-5.16.3-294.el7_6
perl-debuginfo-5.16.3-294.el7_6
perl-core-5.16.3-294.el7_6
perl-macros-5.16.3-294.el7_6
perl-libs-5.16.3-294.el7_6
perl-tests-5.16.3-294.el7_6

noarch
perl-ExtUtils-Embed-1.30-294.el7_6
perl-Module-CoreList-2.76.02-294.el7_6
perl-Object-Accessor-0.42-294.el7_6
perl-ExtUtils-Install-1.58-294.el7_6
perl-Package-Constants-0.02-294.el7_6
perl-Module-Loaded-0.08-294.el7_6
perl-CPAN-1.9800-294.el7_6
perl-IO-Zlib-1.10-294.el7_6
perl-Locale-Maketext-Simple-0.21-294.el7_6
perl-ExtUtils-CBuilder-0.28.2.6-294.el7_6
perl-Pod-Escapes-1.04-294.el7_6

147557 - SuSE Linux 42.3 openSUSE-SU-2019:0068-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-4191, CVE-2018-4197, CVE-2018-4207, CVE-2018-4208, CVE-2018-4209, CVE-2018-4210, CVE-2018-4212, CVE-2018-4213, CVE-2018-4261, CVE-2018-4262, CVE-2018-4263, CVE-2018-4264, CVE-2018-4265, CVE-2018-4266, CVE-2018-4267, CVE-2018-4270, CVE-2018-4272, CVE-2018-4273, CVE-2018-4278, CVE-2018-4284, CVE-2018-4299, CVE-2018-4306, CVE-2018-4309, CVE-2018-4312, CVE-2018-4314, CVE-2018-4315, CVE-2018-4316, CVE-2018-4317, CVE-2018-4318, CVE-2018-4319, CVE-2018-4323, CVE-2018-4328, CVE-2018-4345, CVE-2018-4358, CVE-2018-4359, CVE-2018-4361, CVE-2018-4372, CVE-2018-4373, CVE-2018-4375, CVE-2018-4376, CVE-2018-4378, CVE-2018-4382, CVE-2018-4386, CVE-2018-4392, CVE-2018-4416

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0068-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00068.html

SuSE Linux 42.3

i586
webkit-jsc-4-2.22.4-15.1
webkit2gtk3-plugin-process-gtk2-2.22.4-15.1
libjavascriptcoregtk-4_0-18-debuginfo-2.22.4-15.1
webkit-jsc-4-debuginfo-2.22.4-15.1
webkit2gtk3-minibrowser-debuginfo-2.22.4-15.1
webkit2gtk3-minibrowser-2.22.4-15.1
typelib-1_0-WebKit2-4_0-2.22.4-15.1
libwebkit2gtk-4_0-37-debuginfo-2.22.4-15.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.4-15.1
typelib-1_0-JavaScriptCore-4_0-2.22.4-15.1
webkit2gtk-4_0-injected-bundles-2.22.4-15.1
libwebkit2gtk-4_0-37-2.22.4-15.1
webkit2gtk3-devel-2.22.4-15.1
webkit2gtk3-debugsource-2.22.4-15.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.22.4-15.1
libjavascriptcoregtk-4_0-18-2.22.4-15.1
typelib-1_0-WebKit2WebExtension-4_0-2.22.4-15.1

noarch
libwebkit2gtk3-lang-2.22.4-15.1

x86_64
webkit-jsc-4-2.22.4-15.1
webkit2gtk3-plugin-process-gtk2-2.22.4-15.1
libjavascriptcoregtk-4_0-18-debuginfo-2.22.4-15.1
libjavascriptcoregtk-4_0-18-32bit-2.22.4-15.1
webkit-jsc-4-debuginfo-2.22.4-15.1
webkit2gtk3-minibrowser-debuginfo-2.22.4-15.1
webkit2gtk3-minibrowser-2.22.4-15.1
typelib-1_0-WebKit2-4_0-2.22.4-15.1
libwebkit2gtk-4_0-37-debuginfo-2.22.4-15.1
webkit2gtk-4_0-injected-bundles-debuginfo-2.22.4-15.1
libwebkit2gtk-4_0-37-debuginfo-32bit-2.22.4-15.1
typelib-1_0-JavaScriptCore-4_0-2.22.4-15.1
webkit2gtk-4_0-injected-bundles-2.22.4-15.1
libjavascriptcoregtk-4_0-18-debuginfo-32bit-2.22.4-15.1
libwebkit2gtk-4_0-37-2.22.4-15.1
webkit2gtk3-devel-2.22.4-15.1
libwebkit2gtk-4_0-37-32bit-2.22.4-15.1
webkit2gtk3-debugsource-2.22.4-15.1
webkit2gtk3-plugin-process-gtk2-debuginfo-2.22.4-15.1
libjavascriptcoregtk-4_0-18-2.22.4-15.1
typelib-1_0-WebKit2WebExtension-4_0-2.22.4-15.1

147558 - SuSE Linux 42.3 openSUSE-SU-2019:0066-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5852, CVE-2017-5853, CVE-2017-5854, CVE-2017-5855, CVE-2017-5886, CVE-2017-6840, CVE-2017-6844, CVE-2017-6845, CVE-2017-6847, CVE-2017-7378, CVE-2017-7379, CVE-2017-7380, CVE-2017-7994, CVE-2017-8054, CVE-2017-8787, CVE-2018-5295, CVE-2018-5296, CVE-2018-5308, CVE-2018-5309, CVE-2018-8001

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0066-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00066.html

SuSE Linux 42.3
x86_64
podofo-0.9.6-10.3.1
libpodofo0_9_6-debuginfo-0.9.6-10.3.1
libpodofo-devel-0.9.6-10.3.1
podofo-debuginfo-0.9.6-10.3.1
podofo-debugsource-0.9.6-10.3.1
libpodofo0_9_6-0.9.6-10.3.1

i586
podofo-0.9.6-10.3.1
libpodofo0_9_6-debuginfo-0.9.6-10.3.1
libpodofo-devel-0.9.6-10.3.1
podofo-debuginfo-0.9.6-10.3.1
podofo-debugsource-0.9.6-10.3.1
libpodofo0_9_6-0.9.6-10.3.1

147561 - SuSE SLED 15 SUSE-SU-2019:0133-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20337, CVE-2018-20363, CVE-2018-20364, CVE-2018-20365, CVE-2018-5817, CVE-2018-5818, CVE-2018-5819

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0133-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005050.html

SuSE SLED 15
x86_64
libraw-debugsource-0.18.9-3.8.1
libraw16-debuginfo-0.18.9-3.8.1
libraw-devel-0.18.9-3.8.1
libraw-debuginfo-0.18.9-3.8.1
libraw16-0.18.9-3.8.1

186540 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3864-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10963, CVE-2018-17100, CVE-2018-17101, CVE-2018-18557, CVE-2018-18661, CVE-2018-7456, CVE-2018-8905

Description

The scan detected that the host is missing the following update:
USN-3864-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-January/004736.html

Ubuntu 16.04

libtiff5_4.0.6-1ubuntu0.5
libtiff-tools_4.0.6-1ubuntu0.5

Ubuntu 18.10

libtiff-tools_4.0.9-6ubuntu0.1
libtiff5_4.0.9-6ubuntu0.1

Ubuntu 14.04

libtiff5_4.0.3-7ubuntu0.10
libtiff-tools_4.0.3-7ubuntu0.10

Ubuntu 18.04

libtiff-tools_4.0.9-5ubuntu0.1
libtiff5_4.0.9-5ubuntu0.1

194682 - Fedora Linux 28 FEDORA-2019-348547a32d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-17480, CVE-2018-17481, CVE-2018-18335, CVE-2018-18336, CVE-2018-18337, CVE-2018-18338, CVE-2018-18339, CVE-2018-18340, CVE-2018-18341, CVE-2018-18342, CVE-2018-18343, CVE-2018-18344, CVE-2018-18345, CVE-2018-18346, CVE-2018-18347, CVE-2018-18348, CVE-2018-18349, CVE-2018-18350, CVE-2018-18351, CVE-2018-18352, CVE-2018-18353, CVE-2018-18354, CVE-2018-18355, CVE-2018-18356, CVE-2018-18357, CVE-2018-18358, CVE-2018-18359

Description

The scan detected that the host is missing the following update:
FEDORA-2019-348547a32d

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/2019/1/?count=200&page=3

Fedora Core 28

chromium-71.0.3578.98-1.fc28

194685 - Fedora Linux 29 FEDORA-2019-ae92ca8981 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19664, CVE-2018-20330

Description

The scan detected that the host is missing the following update:
FEDORA-2019-ae92ca8981

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/2019/1/?count=200&page=1

Fedora Core 29

libjpeg-turbo-2.0.0-3.fc29

194690 - Fedora Linux 29 FEDORA-2019-a018522ba3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19664, CVE-2018-20330

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a018522ba3

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/2019/1/?count=200&page=1

Fedora Core 29

mingw-libjpeg-turbo-2.0.0-2.fc29

24642 - Wireshark Multiple Vulnerabilities Prior To 2.6.6

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

Risk Level: Medium

CVE: CVE-2019-5716, CVE-2019-5717, CVE-2019-5718, CVE-2019-5719

Description

Multiple vulnerabilities are present in some versions of Wireshark.

Observation

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

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

194686 - Fedora Linux 28 FEDORA-2018-9dd3f7c013 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10091

Description

The scan detected that the host is missing the following update:
FEDORA-2018-9dd3f7c013

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/2019/1/?count=200&page=3

Fedora Core 28

unrtf-0.21.9-8.fc28

194691 - Fedora Linux 28 FEDORA-2019-c6044b3fce Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12291, CVE-2019-5885

Description

The scan detected that the host is missing the following update:
FEDORA-2019-c6044b3fce

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/2019/1/?count=200&page=1

Fedora Core 28

matrix-synapse-0.34.0.1-2.fc28

194698 - Fedora Linux 29 FEDORA-2019-50cc0c11e9 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14647

Description

The scan detected that the host is missing the following update:
FEDORA-2019-50cc0c11e9

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/2019/1/?count=200&page=2

Fedora Core 29

python36-3.6.8-1.fc29

194700 - Fedora Linux 28 FEDORA-2019-a6511b0eed Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19935

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a6511b0eed

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/2019/1/?count=200&page=2

Fedora Core 28

php-7.2.14-1.fc28

194711 - Fedora Linux 29 FEDORA-2019-aa6036fcb3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19935

Description

The scan detected that the host is missing the following update:
FEDORA-2019-aa6036fcb3

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/2019/1/?count=200&page=2

Fedora Core 29

php-7.2.14-1.fc29

147562 - SuSE SLED 12 SP3, 12 SP4 SUSE-SU-2019:0127-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20363, CVE-2018-20364, CVE-2018-20365, CVE-2018-5817, CVE-2018-5818, CVE-2018-5819

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0127-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005044.html

SuSE SLED 12 SP4
x86_64
libraw9-debuginfo-0.15.4-30.1
libraw-debugsource-0.15.4-30.1
libraw9-0.15.4-30.1

SuSE SLED 12 SP3
x86_64
libraw9-debuginfo-0.15.4-30.1
libraw-debugsource-0.15.4-30.1
libraw9-0.15.4-30.1

147568 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0138-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-5717, CVE-2019-5718, CVE-2019-5719, CVE-2019-5721

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0138-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005055.html

SuSE SLED 12 SP3
x86_64
wireshark-2.4.12-48.39.1
libwireshark9-2.4.12-48.39.1
wireshark-debugsource-2.4.12-48.39.1
libwsutil8-2.4.12-48.39.1
wireshark-gtk-2.4.12-48.39.1
libwscodecs1-debuginfo-2.4.12-48.39.1
libwiretap7-2.4.12-48.39.1
wireshark-gtk-debuginfo-2.4.12-48.39.1
wireshark-debuginfo-2.4.12-48.39.1
libwiretap7-debuginfo-2.4.12-48.39.1
libwscodecs1-2.4.12-48.39.1
libwsutil8-debuginfo-2.4.12-48.39.1
libwireshark9-debuginfo-2.4.12-48.39.1

SuSE SLED 12 SP4
x86_64
wireshark-2.4.12-48.39.1
libwireshark9-2.4.12-48.39.1
wireshark-debugsource-2.4.12-48.39.1
libwsutil8-2.4.12-48.39.1
wireshark-gtk-2.4.12-48.39.1
libwscodecs1-debuginfo-2.4.12-48.39.1
libwiretap7-2.4.12-48.39.1
wireshark-gtk-debuginfo-2.4.12-48.39.1
wireshark-debuginfo-2.4.12-48.39.1
libwiretap7-debuginfo-2.4.12-48.39.1

libwscodecs1-2.4.12-48.39.1
libwsutil8-debuginfo-2.4.12-48.39.1
libwireshark9-debuginfo-2.4.12-48.39.1

SuSE SLES 12 SP4
x86_64
wireshark-2.4.12-48.39.1
libwireshark9-2.4.12-48.39.1
wireshark-debugsource-2.4.12-48.39.1
libwsutil8-2.4.12-48.39.1
wireshark-gtk-2.4.12-48.39.1
libwscodecs1-debuginfo-2.4.12-48.39.1
libwiretap7-2.4.12-48.39.1
wireshark-gtk-debuginfo-2.4.12-48.39.1
wireshark-debuginfo-2.4.12-48.39.1
libwiretap7-debuginfo-2.4.12-48.39.1
libwscodecs1-2.4.12-48.39.1
libwsutil8-debuginfo-2.4.12-48.39.1
libwireshark9-debuginfo-2.4.12-48.39.1

SuSE SLES 12 SP3
x86_64
wireshark-2.4.12-48.39.1
libwireshark9-2.4.12-48.39.1
wireshark-debugsource-2.4.12-48.39.1
libwsutil8-2.4.12-48.39.1
wireshark-gtk-2.4.12-48.39.1
libwscodecs1-debuginfo-2.4.12-48.39.1
libwiretap7-2.4.12-48.39.1
wireshark-gtk-debuginfo-2.4.12-48.39.1
wireshark-debuginfo-2.4.12-48.39.1
libwiretap7-debuginfo-2.4.12-48.39.1
libwscodecs1-2.4.12-48.39.1
libwsutil8-debuginfo-2.4.12-48.39.1
libwireshark9-debuginfo-2.4.12-48.39.1

182891 - FreeBSD joomla3 Vulnerabilitiesw (6aa398d0-1c4d-11e9-96dd-a4badb296695)

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

Risk Level: Medium

CVE: CVE-2019-6261, CVE-2019-6262, CVE-2019-6263, CVE-2019-6264

Description

The scan detected that the host is missing the following update:
joomla3 -- vulnerabilitiesw (6aa398d0-1c4d-11e9-96dd-a4badb296695)

Observation

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

http://www.vuxml.org/freebsd/6aa398d0-1c4d-11e9-96dd-a4badb296695.html

Affected packages:
joomla3 < 3.9.2

194684 - Fedora Linux 28 FEDORA-2019-d4d8af2c22 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20455, CVE-2018-20456, CVE-2018-20457, CVE-2018-20458, CVE-2018-20459, CVE-2018-20460, CVE-2018-20461

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d4d8af2c22

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/2019/1/?count=200&page=2

Fedora Core 28

radare2-3.2.0-1.fc28

194692 - Fedora Linux 29 FEDORA-2019-f812c9fb22 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16862, CVE-2018-18710, CVE-2018-19407, CVE-2018-19824, CVE-2019-3459, CVE-2019-3460, CVE-2019-3701

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f812c9fb22

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/2019/1/?count=200&page=2

Fedora Core 29

kernel-4.19.15-300.fc29
kernel-headers-4.19.15-300.fc29

194699 - Fedora Linux 29 FEDORA-2019-5750ad7485 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20455, CVE-2018-20456, CVE-2018-20457, CVE-2018-20458, CVE-2018-20459, CVE-2018-20460, CVE-2018-20461

Description

The scan detected that the host is missing the following update:
FEDORA-2019-5750ad7485

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/2019/1/?count=200&page=2

Fedora Core 29

radare2-3.2.0-1.fc29

131276 - Debian Linux 9.0 DSA-4371-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3462

Description

The scan detected that the host is missing the following update:
DSA-4371-1

Observation

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

http://www.debian.org/security/2019/dsa-4371

Debian 9.0
all
apt_1.4.9

131277 - Debian Linux 9.0 DSA-4370-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-6338, CVE-2019-6339

Description

The scan detected that the host is missing the following update:
DSA-4370-1

Observation

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

http://www.debian.org/security/2019/dsa-4370

Debian 9.0
all
drupal7_7.52-2+deb9u6

147550 - SuSE Linux 42.3 openSUSE-SU-2019:0061-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-3239

Description

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

openSUSE-SU-2019:0061-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-01/msg00058.html

SuSE Linux 42.3
x86_64
libunwind-devel-1.1-15.3.1
libunwind-debuginfo-1.1-15.3.1
libunwind-debugsource-1.1-15.3.1
libunwind-debuginfo-32bit-1.1-15.3.1
libunwind-32bit-1.1-15.3.1
libunwind-1.1-15.3.1

i586
libunwind-devel-1.1-15.3.1
libunwind-debuginfo-1.1-15.3.1
libunwind-1.1-15.3.1
libunwind-debugsource-1.1-15.3.1

182886 - FreeBSD Gitlab Arbitrary Repo Read In Gitlab Project Import (ff50192c-19eb-11e9-8573-001b217b3468)

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

Risk Level: Low

CVE: CVE-2019-6240

Description

The scan detected that the host is missing the following update:
Gitlab -- Arbitrary repo read in Gitlab project import (ff50192c-19eb-11e9-8573-001b217b3468)

Observation

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

http://www.vuxml.org/freebsd/ff50192c-19eb-11e9-8573-001b217b3468.html

Affected packages:
11.6.0 <= gitlab-ce < 11.6.4
11.5.0 <= gitlab-ce < 11.5.7
8.9.0 <= gitlab-ce < 11.4.14

182887 - FreeBSD www/py-requests Information Disclosure Vulnerability (50ad9a9a-1e28-11e9-98d7-0050562a4d7b)

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:
www/py-requests -- Information disclosure vulnerability (50ad9a9a-1e28-11e9-98d7-0050562a4d7b)

Observation

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

http://www.vuxml.org/freebsd/50ad9a9a-1e28-11e9-98d7-0050562a4d7b.html

Affected packages:
py-requests < 2.20.0

182888 - FreeBSD Helm Client Unpacking Chart That Contains Malicious Content (2a8b79c3-1b6e-11e9-8cf4-1c39475b9f84)

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:
Helm -- client unpacking chart that contains malicious content (2a8b79c3-1b6e-11e9-8cf4-1c39475b9f84)

Observation

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

http://www.vuxml.org/freebsd/2a8b79c3-1b6e-11e9-8cf4-1c39475b9f84.html

Affected packages:
2.0.0 <= helm < 2.12.2

182889 - FreeBSD drupal Drupal Core - Arbitrary PHP Code Execution (e00ed3d9-1c27-11e9-a257-000ffec0b3e1)

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:
drupal -- Drupal core - Arbitrary PHP code execution (e00ed3d9-1c27-11e9-a257-000ffec0b3e1)

Observation

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

http://www.vuxml.org/freebsd/e00ed3d9-1c27-11e9-a257-000ffec0b3e1.html

Affected packages:
drupal7 < 7.63
drupal8 < 8.6.7

182890 - FreeBSD jenkins Multiple Vulnerabilities (debf6353-5753-4e9a-b710-a83ecdd743de)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
jenkins -- multiple vulnerabilities (debf6353-5753-4e9a-b710-a83ecdd743de)

Observation

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

http://www.vuxml.org/freebsd/debf6353-5753-4e9a-b710-a83ecdd743de.html

Affected packages:
jenkins < 2.160
jenkins-lts < 2.150.2

186537 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3861-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-19788

Description

The scan detected that the host is missing the following update:
USN-3861-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-January/004731.html

Ubuntu 16.04

libpolkit-backend-1-0_0.105-14.1ubuntu0.4
policykit-1_0.105-14.1ubuntu0.4

Ubuntu 18.10

libpolkit-backend-1-0_0.105-21ubuntu0.3
policykit-1_0.105-21ubuntu0.3

Ubuntu 14.04

libpolkit-backend-1-0_0.105-4ubuntu3.14.04.5
policykit-1_0.105-4ubuntu3.14.04.5

Ubuntu 18.04

policykit-1_0.105-20ubuntu0.18.04.4
libpolkit-backend-1-0_0.105-20ubuntu0.18.04.4

186541 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3863-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3462

Description

The scan detected that the host is missing the following update:
USN-3863-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-January/004734.html

Ubuntu 16.04

apt_1.2.29ubuntu0.1

Ubuntu 18.10

apt_1.7.0ubuntu0.1

Ubuntu 14.04

apt_1.0.1ubuntu2.19

Ubuntu 18.04

apt_1.6.6ubuntu0.1

194679 - Fedora Linux 28 FEDORA-2019-9eb0ae6296 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20685

Description

The scan detected that the host is missing the following update:
FEDORA-2019-9eb0ae6296

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/2019/1/?count=200&page=1

Fedora Core 28

openssh-7.8p1-4.fc28

194683 - Fedora Linux 28 FEDORA-2019-fb2ce5f6d9 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-2019-fb2ce5f6d9

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/2019/1/?count=200&page=3

Fedora Core 28

php-horde-Horde-Form-2.0.19-1.fc28

194688 - Fedora Linux 28 FEDORA-2019-541a12b809 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-2019-541a12b809

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/2019/1/?count=200&page=2

Fedora Core 28

python3-docs-3.6.8-1.fc28
python3-3.6.8-1.fc28

194693 - Fedora Linux 28 FEDORA-2019-e70c729d8a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1000858

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e70c729d8a

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/2019/1/?count=200&page=1

Fedora Core 28

gnupg2-2.2.12-1.fc28

194694 - Fedora Linux 29 FEDORA-2019-972e3107bd 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-2019-972e3107bd

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/2019/1/?count=200&page=1

Fedora Core 29

gvfs-1.38.1-2.fc29

194695 - Fedora Linux 29 FEDORA-2019-b276ee69a8 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-2019-b276ee69a8

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/2019/1/?count=200&page=2

Fedora Core 29

gitolite3-3.6.11-1.fc29

194696 - Fedora Linux 29 FEDORA-2019-f6ff819834 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20685

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f6ff819834

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/2019/1/?count=200&page=2

Fedora Core 29

openssh-7.9p1-3.fc29

194697 - Fedora Linux 29 FEDORA-2019-8fe9d427f1 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-2019-8fe9d427f1

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/2019/1/?count=200&page=3

Fedora Core 29

php-horde-Horde-Form-2.0.19-1.fc29

194701 - Fedora Linux 28 FEDORA-2019-e6ca5847c7 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3498

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e6ca5847c7

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/2019/1/?count=200&page=3

Fedora Core 28

python-django-2.0.10-1.fc28

194702 - Fedora Linux 28 FEDORA-2019-b6ce519120 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-2019-b6ce519120

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/2019/1/?count=200&page=2

Fedora Core 28

gitolite3-3.6.11-1.fc28

194704 - Fedora Linux 28 FEDORA-2019-b1da89df11 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1116, CVE-2018-19788

Description

The scan detected that the host is missing the following update:
FEDORA-2019-b1da89df11

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/2019/1/?count=200&page=1

Fedora Core 28

polkit-0.115-2.1.fc28

194705 - Fedora Linux 29 FEDORA-2019-41a3fb1d64 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-2019-41a3fb1d64

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/2019/1/?count=200&page=2

Fedora Core 29

electrum-3.2.4-2.fc29

194706 - Fedora Linux 29 FEDORA-2019-4d914f9257 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-5885

Description

The scan detected that the host is missing the following update:
FEDORA-2019-4d914f9257

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/2019/1/?count=200&page=1

Fedora Core 29

matrix-synapse-0.34.0.1-1.fc29

194707 - Fedora Linux 29 FEDORA-2019-e818eaa0ac 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-2019-e818eaa0ac

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/2019/1/?count=200&page=1

Fedora Core 29

syslog-ng-3.17.2-2.fc29

196233 - Red Hat Enterprise Linux RHSA-2019-0095 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2019-0095

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-January/msg00017.html

RHEL6_7S
i386
redhat-release-server-6Server-6.7.0.5.el6_7.3

x86_64

redhat-release-server-6Server-6.7.0.5.el6_7.3

139103 - Oracle Solaris 11.3.36.7.0 Update Is Not Installed (Third Party Components)

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

Risk Level: Low

CVE: CVE-2018-0734, CVE-2018-0735, CVE-2018-5407

Description

The scan detected that the host is missing the following update:
SRU 11.3.36.7.0

Observation

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

https://support.oracle.com/rs?type=doc&id=2492416.1
https://support.oracle.com/epmos/faces/DocumentDisplay?
_afrLoop=507462766511768&id=1448883.1&_afrWindowMode=0&_adf.ctrl-state=98kg3qcn0_33#aref_section26

194680 - Fedora Linux 29 FEDORA-2019-a8ffcff7ee Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-0495, CVE-2018-0734, CVE-2018-0735

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a8ffcff7ee

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/2019/1/?count=200&page=2

Fedora Core 29

openssl-1.1.1a-1.fc29

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.

24541 - (APSB18-41) Vulnerabilities In Adobe Acrobat and Reader

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

Risk Level: High

CVE: CVE-2018-12830, CVE-2018-15984, CVE-2018-15985, CVE-2018-15986, CVE-2018-15987, CVE-2018-15988, CVE-2018-15989, CVE-2018-15990, CVE-2018-15991, CVE-2018-15992, CVE-2018-15993, CVE-2018-15994, CVE-2018-15995, CVE-2018-15996, CVE-2018-15997, CVE-2018-15998, CVE-2018-15999, CVE-2018-16000, CVE-2018-16001, CVE-2018-16002, CVE-2018-16003, CVE-2018-16004, CVE-2018-16005, CVE-2018-16006, CVE-2018-16007, CVE-2018-16008, CVE-2018-16009, CVE-2018-16010, CVE-2018-16011, CVE-2018-16012, CVE-2018-16013, CVE-2018-16014, CVE-2018-16015, CVE-2018-16016, CVE-2018-

16017, CVE-2018-16018, CVE-2018-16019, CVE-2018-16020, CVE-2018-16021, CVE-2018-16022, CVE-2018-16023, CVE-2018-16024, CVE-2018-16025, CVE-2018-16026, CVE-2018-16027, CVE-2018-16028, CVE-2018-16029, CVE-2018-16030, CVE-2018-16031, CVE-2018-16032, CVE-2018-16033, CVE-2018-16034, CVE-2018-16035, CVE-2018-16036, CVE-2018-16037, CVE-2018-16038, CVE-2018-16039, CVE-2018-16040, CVE-2018-16041, CVE-2018-16042, CVE-2018-16043, CVE-2018-16044, CVE-2018-16045, CVE-2018-16046, CVE-2018-16047, CVE-2018-19698, CVE-2018-19699, CVE-2018-19700, CVE-2018-19701, CVE-2018-19702, CVE-2018-19703, CVE-2018-19704, CVE-2018-19705, CVE-2018-19706, CVE-2018-19707, CVE-2018-19708, CVE-2018-19709, CVE-2018-19710, CVE-2018-19711, CVE-2018-19712, CVE-2018-19713, CVE-2018-19714, CVE-2018-19715, CVE-2018-19716, CVE-2018-19717, CVE-2018-19719, CVE-2018-19720

Update Details

Risk is updated

88975 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-249-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14618

Update Details

Risk is updated

131197 - Debian Linux 9.0 DSA-4286-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14618

Update Details

Risk is updated

139011 - Oracle Solaris 11.2 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2011-4320, CVE-2012-0804, CVE-2012-2369, CVE-2012-2751, CVE-2012-3461, CVE-2012-3479, CVE-2012-6152, CVE-2013-0179, CVE-2013-0271, CVE-2013-0272, CVE-2013-0273, CVE-2013-0274, CVE-2013-0346, CVE-2013-0913, CVE-2013-1915, CVE-2013-1969, CVE-2013-2168, CVE-2013-2765, CVE-2013-4164, CVE-2013-4243, CVE-2013-4244, CVE-2013-4276, CVE-2013-4287, CVE-2013-4351, CVE-2013-4353, CVE-2013-4363, CVE-2013-4402, CVE-2013-4761, CVE-2013-4885, CVE-2013-4956, CVE-2013-6169, CVE-2013-6449, CVE-2013-6450, CVE-2013-6477, CVE-2013-6478, CVE-2013-6479, CVE-2013-6481, CVE-2013-6482, CVE-2013-6483, CVE-2013-6484, CVE-2013-6485, CVE-2013-6486, CVE-2013-6487, CVE-2013-6489, CVE-2013-6490, CVE-2014-0020, CVE-2014-0076, CVE-2014-0160, CVE-2014-0472, CVE-2014-0473, CVE-2014-0474, CVE-2014-1932, CVE-2014-1933, CVE-2014-1947, CVE-2014-1958, CVE-2014-2030, CVE-2014-2828, CVE-2014-2907, CVE-2014-4275, CVE-2014-4276, CVE-2014-4277, CVE-2014-4280, CVE-2014-4282, CVE-2014-4283, CVE-2014-4284, CVE-2014-6470, CVE-2014-6473, CVE-2014-6490, CVE-2014-6497, CVE-2014-6501, CVE-2014-6508, CVE-2015-0375, CVE-2015-2577, CVE-2019-2543, CVE-2019-2544

Update Details

CVE is updated

139061 - Oracle Solaris 11.3.9.4.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2014-9679, CVE-2014-9848, CVE-2014-9849, CVE-2014-9852, CVE-2014-9853, CVE-2014-9854, CVE-2015-1547, CVE-2015-2806, CVE-2015-5223, CVE-2015-5295, CVE-2015-7546, CVE-2015-8665, CVE-2015-8683, CVE-2015-8781, CVE-2015-8782,

CVE-2015-8783, CVE-2015-8784, CVE-2015-8786, CVE-2015-8853, CVE-2015-8895, CVE-2015-8896, CVE-2015-8897, CVE-2015-8898, CVE-2015-8959, CVE-2016-0737, CVE-2016-0738, CVE-2016-10252, CVE-2016-2102176, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176, CVE-2016-2381, CVE-2016-2512, CVE-2016-2513, CVE-2016-3115, CVE-2016-3714, CVE-2016-3715, CVE-2016-3716, CVE-2016-3717, CVE-2016-3718, CVE-2016-4006, CVE-2016-4078, CVE-2016-4079, CVE-2016-4080, CVE-2016-4081, CVE-2016-4082, CVE-2016-4085, CVE-2016-4562, CVE-2016-4563, CVE-2016-4564, CVE-2016-5118, CVE-2016-5239, CVE-2016-5359, CVE-2016-5452, CVE-2016-5454, CVE-2016-5471, CVE-2017-10042

Update Details

CVE is updated

139100 - Oracle Solaris 11.4 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2016-6352, CVE-2016-7044, CVE-2016-7045, CVE-2016-7162, CVE-2016-7163, CVE-2016-7166, CVE-2016-7445, CVE-2016-7553, CVE-2016-7957, CVE-2016-7958, CVE-2016-7976, CVE-2016-7977, CVE-2016-7978, CVE-2016-7979, CVE-2016-8864, CVE-2016-9013, CVE-2016-9014, CVE-2016-9179, CVE-2016-9185, CVE-2017-10788, CVE-2017-11109, CVE-2017-11112, CVE-2017-11113, 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-2017-12982, CVE-2017-14039, CVE-2017-14040, CVE-2017-14041, CVE-2017-14151, CVE-2017-14152, CVE-2017-14164, CVE-2017-2292, CVE-2017-2592, CVE-2017-3135, CVE-2017-3136, CVE-2017-3137, CVE-2017-3138, CVE-2017-3140, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5448, CVE-2017-5449, CVE-2017-5451, CVE-2017-5454, CVE-2017-5455, CVE-2017-5456, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5468, CVE-2017-5469, CVE-2017-5715, CVE-2017-5754, CVE-2017-7407, CVE-2017-7511, CVE-2017-7555, CVE-2017-8291, CVE-2017-8786, CVE-2017-8932, CVE-2017-9083, CVE-2017-9110, CVE-2017-9111, CVE-2017-9112, CVE-2017-9113, CVE-2017-9114, CVE-2017-9115, CVE-2017-9116, CVE-2017-9406, CVE-2017-9408, CVE-2018-1166, CVE-2018-3263, CVE-2018-3264, CVE-2018-3265, CVE-2018-3266, CVE-2018-3267, CVE-2018-3268, CVE-2018-3269, CVE-2018-3270, CVE-2018-3271, CVE-2018-3272, CVE-2018-3273, CVE-2018-3274, CVE-2018-3275, CVE-2018-3665, CVE-2019-2545

Update Details

CVE is updated

147087 - SuSE SLES 11 SP4 SUSE-SU-2018:2717-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14618

Update Details

Risk is updated

147092 - SuSE Linux 42.3 openSUSE-SU-2018:2736-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14618

Update Details

Risk is updated

147094 - SuSE Linux 15.0 openSUSE-SU-2018:2731-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14618

Update Details

Risk is updated

147103 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:2715-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14618

Update Details

Risk is updated

171046 - Amazon Linux AMI ALAS-2018-1112 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14618

Update Details

Risk is updated

182785 - FreeBSD curl Password Overflow Vulnerability (f4d638b9-e6e5-4dbe-8c70-571dbc116174)

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

Risk Level: High

CVE: CVE-2018-14618

Update Details

Risk is updated

194183 - Fedora Linux 29 FEDORA-2018-7f83032de6 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-14618

Update Details

Risk is updated

24611 - (APSB19-02) Multiple vulnerabilities In Adobe Acrobat and Reader

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

Risk Level: High

CVE: CVE-2018-16011, CVE-2018-16018

Update Details

Risk is updated

135230 - Oracle Solaris 11.4.3.5.0 Update Is Not Installed (CVE-2019-2437)

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

Risk Level: High

CVE: CVE-2019-2437

Update Details

Risk is updated

139009 - Oracle Solaris 11.1.19.6.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2012-3544, CVE-2012-4037, CVE-2013-0200, CVE-2013-1571, CVE-2013-4248, CVE-2013-4286, CVE-2013-4322, CVE-2013-4590, CVE-2013-6420, CVE-2013-6438, CVE-2013-6712, CVE-2014-0033, CVE-2014-0098, CVE-2014-0591, CVE-2014-1943, CVE-2014-2270, CVE-2014-2281, CVE-2014-2282, CVE-2014-2283, CVE-2014-4239, CVE-2019-2543, CVE-2019-2544

Update Details

CVE is updated

139086 - Oracle Solaris 11.3.17.5.0 Update Is Not Installed (Third Party Components)

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

Risk Level: High

CVE: CVE-2013-7447, CVE-2015-7674, CVE-2015-8875, CVE-2016-0634, CVE-2016-0736, CVE-2016-10002, CVE-2016-10003, CVE-2016-10109, CVE-2016-10167, CVE-2016-10168, CVE-2016-2123, CVE-2016-2125, CVE-2016-2126, CVE-2016-2161, CVE-2016-3191, CVE-2016-4975, CVE-2016-7055, CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-7543, CVE-2016-7799, CVE-2016-7906, CVE-2016-8740, CVE-2016-8743, CVE-2016-8862, CVE-2016-9131, CVE-2016-9147, CVE-2016-9298, CVE-2016-9310, CVE-2016-9311, CVE-2016-9312, CVE-2016-9401, CVE-2016-9444, CVE-2016-9556, CVE-2016-9559, CVE-2016-9844, CVE-2016-9893, CVE-2016-9895, CVE-2016-9897, CVE-2016-9898, CVE-2016-9899, CVE-2016-9900, CVE-2016-9904, CVE-2016-9905, CVE-2017-3474, CVE-2017-3497, CVE-2017-3551, CVE-2017-3731, CVE-2017-3732, CVE-2017-5373, CVE-2017-5375, CVE-2017-5376, CVE-2017-5378, CVE-2017-5380, CVE-2017-5383, CVE-2017-5386, CVE-2017-5390, CVE-2017-5396

Update Details

CVE is updated

131268 - Debian Linux 9.0 DSA-4362-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-12405, CVE-2018-17466, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18498

Update Details

Risk is updated CVE is updated

135233 - Oracle Solaris 11.1.19.6.0 Update Is Not Installed (CVE-2019-2543)

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

Risk Level: Medium

CVE: CVE-2019-2543

Update Details

Risk is updated

171056 - Amazon Linux AMI ALAS-2018-1132 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14647

Update Details

FASLScript is updated

147228 - SuSE Linux 15.0 openSUSE-SU-2018:3185-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11763

Update Details

Risk is updated

147299 - SuSE SLES 12 SP3 SUSE-SU-2018:3582-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11763

Update Details

Risk is updated

147334 - SuSE Linux 42.3 openSUSE-SU-2018:3713-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11763

Update Details

Risk is updated

147436 - SuSE SLES 12 SP4 SUSE-SU-2018:3582-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11763

Update Details

Risk is updated

171052 - Amazon Linux AMI ALAS-2018-1104 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-11763

Update Details
Risk is updated

182808 - FreeBSD Apache Denial Of Service Vulnerability In HTTP/2 (e182c076-c189-11e8-a6d2-b499baebfeaf)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-11763

Update Details
Risk is updated

186359 - Ubuntu Linux 18.04 USN-3746-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-0501

Update Details
Risk is updated

194317 - Fedora Linux 28 FEDORA-2018-6ffb18592f Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-11763

Update Details
Risk is updated

194368 - Fedora Linux 29 FEDORA-2018-9cdbb641f9 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-11763

Update Details
Risk is updated

135234 - Oracle Solaris 11.1.19.6.0 Update Is Not Installed (CVE-2019-2544)

Category: SSH Module -> NonIntrusive -> Solaris Patches and Hotfixes
Risk Level: Low
CVE: CVE-2019-2544

Update Details
Risk is updated

145650 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0409-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-7056

Update Details

Risk is updated

182259 - FreeBSD openssl Timing Attack Vulnerability (7caebe30-d7f1-11e6-a9a5-b499baebfeaf)

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

Risk Level: Low

CVE: CVE-2016-7056

Update Details

Risk is updated

HOW TO UPDATE

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

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

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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