2018-MAY-31
FSL version 7.6.26

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

23609 - (SB10235) McAfee Network Data Loss Prevention Remote Code Execution Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-10229

Description

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

Observation

McAfee Network Data Loss Prevention monitors and prevents risky user behavior that can lead to a sensitive data breach.

A vulnerability is present in some versions of McAfee Network Data Loss Prevention. The flaw lies in the OS kernel. Successful exploitation could allow an attacker to remotely execute arbitrary code. Exploitation requires an attacker to send malicious UDP traffic to trigger the flaw in the recv system call.

23617 - (APSB18-17) Remote Code Execution Vulnerability In Adobe Photoshop CC

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

Risk Level: High

CVE: CVE-2018-4946

Description

A vulnerability is present in some versions of Adobe Photoshop CC.

Observation

Adobe Photoshop CC is a product for media editing and management.

A vulnerability is present in some versions of Adobe Photoshop CC. The flaw lies in an undetermined component. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

23622 - (APSB18-17) Remote Code Execution Vulnerability In Adobe Photoshop CC

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-4946

Description

A vulnerability is present in some versions of Adobe Photoshop CC.

Observation

Adobe Photoshop CC is a product for media editing and management.

A vulnerability is present in some versions of Adobe Photoshop CC. The flaw lies in an undetermined component. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

23628 - IBM WebSphere Application Server Multiple Vulnerabilities (swg22015347)

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

Risk Level: High

CVE: CVE-2016-0702, CVE-2016-0705, CVE-2017-3732, CVE-2017-3736, CVE-2018-1426, CVE-2018-1427, CVE-2018-1447

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server.

Observation

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

Multiple vulnerabilities are present in some versions of IBM WebSphere Application Server. The flaw lies in the GSKit component. Successful exploitation could allow a remote attacker to obtain sensitive information or lead to a denial-of-service condition.

96062 - Red Hat Enterprise Linux RHSA-2018-1737 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18017, CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1737

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00126.html

RHEL7_3S
noarch
kernel-abi-whitelists-3.10.0-514.51.1.el7
kernel-doc-3.10.0-514.51.1.el7

x86_64
kernel-devel-3.10.0-514.51.1.el7
kernel-3.10.0-514.51.1.el7
kernel-debug-debuginfo-3.10.0-514.51.1.el7
kernel-tools-libs-devel-3.10.0-514.51.1.el7
kernel-debuginfo-common-x86_64-3.10.0-514.51.1.el7
kernel-tools-3.10.0-514.51.1.el7
kernel-debug-3.10.0-514.51.1.el7
perf-debuginfo-3.10.0-514.51.1.el7
python-perf-3.10.0-514.51.1.el7
kernel-tools-libs-3.10.0-514.51.1.el7
python-perf-debuginfo-3.10.0-514.51.1.el7
kernel-debug-devel-3.10.0-514.51.1.el7
kernel-headers-3.10.0-514.51.1.el7

kernel-debuginfo-3.10.0-514.51.1.el7
perf-3.10.0-514.51.1.el7
kernel-tools-debuginfo-3.10.0-514.51.1.el7

23626 - (HPESBHF03769) HPE Integrated Lights-Out Vulnerability

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

Risk Level: High

CVE: CVE-2017-12542

Description

A vulnerability is present in some versions of HPE Integrated Lights-Out.

Observation

HPE Integrated Lights-Out is a Hewlett-Packard proprietary embedded server management technology.

A vulnerability is present in some versions of HPE Integrated Lights-Out. The flaw lies in an unknown component. Successful exploitation could allow a remote attacker to execute arbitrary code or bypass authentication security measures.

193732 - Fedora Linux 26 FEDORA-2018-7cd077ddd3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10664, CVE-2017-11334, CVE-2017-12135, CVE-2017-12136, CVE-2017-12137, CVE-2017-12855, CVE-2017-13672, CVE-2017-13673, CVE-2017-14316, CVE-2017-14317, CVE-2017-14318, CVE-2017-14319, CVE-2017-15588, CVE-2017-15589, CVE-2017-15590, CVE-2017-15591, CVE-2017-15592, CVE-2017-15593, CVE-2017-15594, CVE-2017-15595, CVE-2017-15597, CVE-2017-17044, CVE-2017-17045, CVE-2017-17046, CVE-2017-5579, CVE-2017-7718, CVE-2017-8309, CVE-2017-8379, CVE-2017-9330, CVE-2017-9524, CVE-2018-10981, CVE-2018-10982, CVE-2018-7540, CVE-2018-7541, CVE-2018-7542, CVE-2018-8897

Description

The scan detected that the host is missing the following update:
FEDORA-2018-7cd077ddd3

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/2018/5/?count=200&page=1

Fedora Core 26

xen-4.8.3-5.fc26

193740 - Fedora Linux 27 FEDORA-2018-9c88c32d15 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000408, CVE-2017-1000409, CVE-2017-15804, CVE-2017-16997, CVE-2017-17426, CVE-2018-1000001, CVE-2018-6485, CVE-2018-6551

Description

The scan detected that the host is missing the following update:
FEDORA-2018-9c88c32d15

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/2018/5/?count=200&page=2

Fedora Core 27

glibc-2.26-28.fc27

23632 - (HPESBHF03831) HPE Integrated Lights-Out Remote Password Hash Vulnerability

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

Risk Level: High

CVE: CVE-2013-4786

Description

A vulnerability is present in some versions of HPE Integrated Lights-Out.

Observation

HPE Integrated Lights-Out is a Hewlett-Packard proprietary embedded server management technology.

A vulnerability is present in some versions of HPE Integrated Lights-Out. The flaw lies in the IPMI 2.0 authentication process. Successful exploitation could allow a remote attacker to bypass security measure and gain unauthorized privileges and unauthorized access to privileged information.

193733 - Fedora Linux 26 FEDORA-2018-6367a17aa3 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000111, CVE-2017-1000112, CVE-2017-1000251, CVE-2017-1000255, CVE-2017-1000405, CVE-2017-10810, CVE-2017-12134, CVE-2017-12153, CVE-2017-12154, CVE-2017-12190, CVE-2017-12193, CVE-2017-13693, CVE-2017-13694, CVE-2017-13695, CVE-2017-14051, CVE-2017-14497, CVE-2017-14954, CVE-2017-15115, CVE-2017-15265, CVE-2017-16532, CVE-2017-16538, CVE-2017-16644, CVE-2017-16647, CVE-2017-16649, CVE-2017-16650, CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-17558, CVE-2017-17712, CVE-2017-17741, CVE-2017-17852, CVE-2017-17853, CVE-2017-17854, CVE-2017-17855, CVE-2017-17856, CVE-2017-17857, CVE-2017-17862, CVE-2017-17863, CVE-2017-17864, CVE-2017-18232, CVE-2017-5123, CVE-2017-7533, CVE-2017-7558, CVE-2017-8824, CVE-2018-1000004, CVE-2018-1000026, CVE-2018-10021, CVE-2018-10322, CVE-2018-10323, CVE-2018-1065, CVE-2018-1108, CVE-2018-1120, CVE-2018-3639, CVE-2018-5332, CVE-2018-5333, CVE-2018-5344, CVE-2018-5750, CVE-2018-5803, CVE-2018-7757, CVE-2018-7995, CVE-2018-8043

Description

The scan detected that the host is missing the following update:
FEDORA-2018-6367a17aa3

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/2018/5/?count=200&page=1

Fedora Core 26

kernel-4.16.11-100.fc26

23603 - IBM WebSphere Service Registry and Repository Multiple Vulnerabilities (swg22013955)

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

Risk Level: High

CVE: CVE-2018-2579, CVE-2018-2602, CVE-2018-2603, CVE-2018-2633

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere Service Registry and Repository

Observation

IBM WebSphere Service Registry and Repository is a product for enterprise's service oriented architecture applications.

Multiple vulnerabilities are present in some versions of IBM WebSphere Service Registry and Repository. The flaws lie in IBM Java SDK version 6, a subcomponent of the IBM WebSphere Application Server software dependency. Successful exploitation could allow an unauthenticated remote attacker to bypass intended access restrictions, retrieve sensitive information or impact availability.

23604 - IBM WebSphere Service Registry and Repository Multiple Vulnerabilities (swg22013955)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-2579, CVE-2018-2602, CVE-2018-2603, CVE-2018-2633

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere Service Registry and Repository

Observation

IBM WebSphere Service Registry and Repository is a product for enterprise's service oriented architecture applications.

Multiple vulnerabilities are present in some versions of IBM WebSphere Service Registry and Repository. The flaws lie in IBM Java SDK version 6, a subcomponent of the IBM WebSphere Application Server software dependency. Successful exploitation could allow an unauthenticated remote attacker to bypass intended access restrictions, retrieve sensitive information or impact availability.

23616 - (HPESBGN03767) HPE Operations Orchestration Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2017-8994

Description

A remote code execution vulnerability is present in some versions of HPE Operations Orchestration.

Observation

HP Operations Orchestration is a product for IT automated tasks coordination.

A remote code execution vulnerability is present in some versions of HPE Operations Orchestration. The flaw lies in an undetermined component. Successful exploitation could allow a remote attacker to execute arbitrary code.

23623 - Advantech WebAccess HMI Designer Multiple Vulnerabilities Prior To 2.1.7.32 (ICSA-18-114-03)

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

Risk Level: High

CVE: CVE-2018-8833, CVE-2018-8835, CVE-2018-8837

Description

Multiple vulnerabilities are present in some versions of Advantech WebAccess HMI Designer.

Observation

Advantech WebAccess HMI Designer is powerful intuitive software to create total solutions for Human Machine Interface products.

Multiple vulnerabilities are present in some versions of Advantech WebAccess HMI Designer. The flaws lie in how Advantech WebAccess HMI Designer manage .pm3 files. Successful exploitation by an user could result in remote code execution.

88948 - Slackware Linux 14.2 SSA:2018-142-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000004, CVE-2018-1092

Description

The scan detected that the host is missing the following update:
SSA:2018-142-01

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=2018&m=slackware-security.696300

Slackware 14.2
i586
kernel-modules-4.4.132-i586-1
kernel-generic-4.4.132-i586-1
kernel-huge-4.4.132-i586-1

i686
kernel-huge-smp-4.4.132_smp-i686-1
kernel-generic-smp-4.4.132_smp-i686-1
kernel-modules-smp-4.4.132_smp-i686-1

noarch
kernel-firmware-20180518_2a9b2cf-noarch-1
kernel-source-4.4.132-noarch-1
kernel-source-4.4.132_smp-noarch-1

x86_64
kernel-modules-4.4.132-x86_64-1
kernel-generic-4.4.132-x86_64-1
kernel-huge-4.4.132-x86_64-1

96057 - Red Hat Enterprise Linux RHSA-2018-1701 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000140

Description

The scan detected that the host is missing the following update:
RHSA-2018-1701

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00106.html

RHEL6_6S
x86_64
librelp-1.2.7-3.el6_6.1
librelp-debuginfo-1.2.7-3.el6_6.1
librelp-devel-1.2.7-3.el6_6.1

96058 - Red Hat Enterprise Linux RHSA-2018-1702 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000140

Description

The scan detected that the host is missing the following update:
RHSA-2018-1702

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00109.html

RHEL6_7S
i386
librelp-debuginfo-1.2.7-3.el6_7.1
librelp-1.2.7-3.el6_7.1
librelp-devel-1.2.7-3.el6_7.1

x86_64
librelp-debuginfo-1.2.7-3.el6_7.1
librelp-1.2.7-3.el6_7.1
librelp-devel-1.2.7-3.el6_7.1

96059 - Red Hat Enterprise Linux RHSA-2018-1638 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1638

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00121.html

RHEL6_7S
i386
kernel-headers-2.6.32-573.55.4.el6
python-perf-debuginfo-2.6.32-573.55.4.el6
kernel-debuginfo-2.6.32-573.55.4.el6
kernel-2.6.32-573.55.4.el6
kernel-debug-debuginfo-2.6.32-573.55.4.el6
perf-2.6.32-573.55.4.el6
kernel-debug-2.6.32-573.55.4.el6
perf-debuginfo-2.6.32-573.55.4.el6
kernel-debug-devel-2.6.32-573.55.4.el6
python-perf-2.6.32-573.55.4.el6
kernel-debuginfo-common-i686-2.6.32-573.55.4.el6
kernel-devel-2.6.32-573.55.4.el6

noarch
kernel-firmware-2.6.32-573.55.4.el6
kernel-doc-2.6.32-573.55.4.el6
kernel-abi-whitelists-2.6.32-573.55.4.el6

x86_64
kernel-debug-debuginfo-2.6.32-573.55.4.el6
kernel-headers-2.6.32-573.55.4.el6
kernel-debuginfo-common-x86_64-2.6.32-573.55.4.el6
kernel-devel-2.6.32-573.55.4.el6
python-perf-2.6.32-573.55.4.el6
python-perf-debuginfo-2.6.32-573.55.4.el6
perf-2.6.32-573.55.4.el6
kernel-debuginfo-2.6.32-573.55.4.el6
perf-debuginfo-2.6.32-573.55.4.el6
kernel-debug-2.6.32-573.55.4.el6
kernel-debuginfo-common-i686-2.6.32-573.55.4.el6
kernel-2.6.32-573.55.4.el6
kernel-debug-devel-2.6.32-573.55.4.el6

96060 - Red Hat Enterprise Linux RHSA-2018-1700 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1124, CVE-2018-1126

Description

The scan detected that the host is missing the following update:
RHSA-2018-1700

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00107.html

RHEL7D
x86_64
procps-ng-i18n-3.3.10-17.el7_5.2
procps-ng-devel-3.3.10-17.el7_5.2
procps-ng-3.3.10-17.el7_5.2

procps-ng-debuginfo-3.3.10-17.el7_5.2

RHEL7S
x86_64
procps-ng-i18n-3.3.10-17.el7_5.2
procps-ng-devel-3.3.10-17.el7_5.2
procps-ng-3.3.10-17.el7_5.2
procps-ng-debuginfo-3.3.10-17.el7_5.2

RHEL7WS
x86_64
procps-ng-i18n-3.3.10-17.el7_5.2
procps-ng-devel-3.3.10-17.el7_5.2
procps-ng-3.3.10-17.el7_5.2
procps-ng-debuginfo-3.3.10-17.el7_5.2

96063 - Red Hat Enterprise Linux RHSA-2018-1707 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000140

Description

The scan detected that the host is missing the following update:
RHSA-2018-1707

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00111.html

RHEL7_3S
x86_64
librelp-devel-1.2.0-4.el7_3
librelp-1.2.0-4.el7_3
librelp-debuginfo-1.2.0-4.el7_3

96064 - Red Hat Enterprise Linux RHSA-2018-1640 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1640

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00124.html

RHEL6_5S
x86_64

kernel-debug-2.6.32-431.89.4.el6
kernel-devel-2.6.32-431.89.4.el6
python-perf-debuginfo-2.6.32-431.89.4.el6
kernel-debug-devel-2.6.32-431.89.4.el6
python-perf-2.6.32-431.89.4.el6
kernel-debuginfo-common-x86_64-2.6.32-431.89.4.el6
kernel-2.6.32-431.89.4.el6
kernel-headers-2.6.32-431.89.4.el6
kernel-debug-debuginfo-2.6.32-431.89.4.el6
perf-2.6.32-431.89.4.el6
perf-debuginfo-2.6.32-431.89.4.el6
kernel-debuginfo-2.6.32-431.89.4.el6

noarch
kernel-firmware-2.6.32-431.89.4.el6
kernel-doc-2.6.32-431.89.4.el6
kernel-abi-whitelists-2.6.32-431.89.4.el6

96065 - Red Hat Enterprise Linux RHSA-2018-1641 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1641

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00122.html

RHEL6_4S
x86_64
kernel-debug-2.6.32-358.88.4.el6
perf-debuginfo-2.6.32-358.88.4.el6
kernel-debuginfo-2.6.32-358.88.4.el6
kernel-devel-2.6.32-358.88.4.el6
python-perf-debuginfo-2.6.32-358.88.4.el6
kernel-debug-debuginfo-2.6.32-358.88.4.el6
perf-2.6.32-358.88.4.el6
kernel-debuginfo-common-x86_64-2.6.32-358.88.4.el6
kernel-headers-2.6.32-358.88.4.el6
kernel-2.6.32-358.88.4.el6
python-perf-2.6.32-358.88.4.el6
kernel-debug-devel-2.6.32-358.88.4.el6

noarch
kernel-firmware-2.6.32-358.88.4.el6
kernel-doc-2.6.32-358.88.4.el6

96066 - Red Hat Enterprise Linux RHSA-2018-1725 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5159, CVE-2018-5161, CVE-2018-5162, CVE-2018-5168, CVE-2018-5170, CVE-2018-5178, CVE-2018-5183, CVE-2018-5184, CVE-2018-5185

Description

The scan detected that the host is missing the following update:
RHSA-2018-1725

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00119.html

RHEL7D
x86_64
thunderbird-52.8.0-1.el7_5
thunderbird-debuginfo-52.8.0-1.el7_5

RHEL7S
x86_64
thunderbird-52.8.0-1.el7_5
thunderbird-debuginfo-52.8.0-1.el7_5

RHEL7WS
x86_64
thunderbird-52.8.0-1.el7_5
thunderbird-debuginfo-52.8.0-1.el7_5

96067 - Red Hat Enterprise Linux RHSA-2018-1726 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5159, CVE-2018-5161, CVE-2018-5162, CVE-2018-5168, CVE-2018-5170, CVE-2018-5178, CVE-2018-5183, CVE-2018-5184, CVE-2018-5185

Description

The scan detected that the host is missing the following update:
RHSA-2018-1726

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00120.html

RHEL6S
i386
thunderbird-52.8.0-2.el6_9
thunderbird-debuginfo-52.8.0-2.el6_9

x86_64
thunderbird-52.8.0-2.el6_9
thunderbird-debuginfo-52.8.0-2.el6_9

RHEL6D
x86_64
thunderbird-52.8.0-2.el6_9

thunderbird-debuginfo-52.8.0-2.el6_9

i386
thunderbird-52.8.0-2.el6_9
thunderbird-debuginfo-52.8.0-2.el6_9

RHEL6WS
x86_64
thunderbird-52.8.0-2.el6_9
thunderbird-debuginfo-52.8.0-2.el6_9

i386
thunderbird-52.8.0-2.el6_9
thunderbird-debuginfo-52.8.0-2.el6_9

96068 - Red Hat Enterprise Linux RHSA-2018-1639 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
RHSA-2018-1639

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00123.html

RHEL6_6S
x86_64
perf-debuginfo-2.6.32-504.69.3.el6
kernel-debuginfo-common-x86_64-2.6.32-504.69.3.el6
kernel-debug-debuginfo-2.6.32-504.69.3.el6
python-perf-2.6.32-504.69.3.el6
kernel-debug-2.6.32-504.69.3.el6
kernel-debuginfo-2.6.32-504.69.3.el6
kernel-2.6.32-504.69.3.el6
perf-2.6.32-504.69.3.el6
python-perf-debuginfo-2.6.32-504.69.3.el6
kernel-devel-2.6.32-504.69.3.el6
kernel-debug-devel-2.6.32-504.69.3.el6
kernel-headers-2.6.32-504.69.3.el6

noarch
kernel-firmware-2.6.32-504.69.3.el6
kernel-abi-whitelists-2.6.32-504.69.3.el6
kernel-doc-2.6.32-504.69.3.el6

146704 - SuSE Linux 42.3 openSUSE-SU-2018:1419-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1419-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00111.html

SuSE Linux 42.3
i586
readline-devel-6.3-83.6.1
libreadline6-6.3-83.6.1
bash-devel-4.3-83.6.1
bash-loadables-debuginfo-4.3-83.6.1
libreadline6-debuginfo-6.3-83.6.1
bash-debugsource-4.3-83.6.1
bash-4.3-83.6.1
bash-loadables-4.3-83.6.1
bash-debuginfo-4.3-83.6.1

noarch
readline-doc-6.3-83.6.1
bash-doc-4.3-83.6.1
bash-lang-4.3-83.6.1

x86_64
readline-devel-6.3-83.6.1
bash-debuginfo-4.3-83.6.1
libreadline6-debuginfo-6.3-83.6.1
libreadline6-6.3-83.6.1
libreadline6-debuginfo-32bit-6.3-83.6.1
bash-debuginfo-32bit-4.3-83.6.1
bash-loadables-debuginfo-4.3-83.6.1
bash-devel-4.3-83.6.1
bash-debugsource-4.3-83.6.1
bash-loadables-4.3-83.6.1
bash-4.3-83.6.1
readline-devel-32bit-6.3-83.6.1
libreadline6-32bit-6.3-83.6.1

146705 - SuSE SLES 11 SP4 SUSE-SU-2018:1367-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-0494

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1367-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004071.html

SuSE SLES 11 SP4
i586
wget-1.11.4-1.41.3.1

x86_64
wget-1.11.4-1.41.3.1

146706 - SuSE Linux 42.3 openSUSE-SU-2018:1439-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18271

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1439-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00129.html

SuSE Linux 42.3
x86_64
GraphicsMagick-debugsource-1.3.25-90.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-90.1
libGraphicsMagick3-config-1.3.25-90.1
GraphicsMagick-debuginfo-1.3.25-90.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-90.1
GraphicsMagick-1.3.25-90.1
perl-GraphicsMagick-debuginfo-1.3.25-90.1
libGraphicsMagick-Q16-3-1.3.25-90.1
libGraphicsMagick++-devel-1.3.25-90.1
libGraphicsMagick++-Q16-12-1.3.25-90.1
GraphicsMagick-devel-1.3.25-90.1
libGraphicsMagickWand-Q16-2-1.3.25-90.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-90.1
perl-GraphicsMagick-1.3.25-90.1

i586
GraphicsMagick-debugsource-1.3.25-90.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.25-90.1
libGraphicsMagick3-config-1.3.25-90.1
GraphicsMagick-debuginfo-1.3.25-90.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.25-90.1
GraphicsMagick-1.3.25-90.1
perl-GraphicsMagick-debuginfo-1.3.25-90.1
libGraphicsMagick-Q16-3-1.3.25-90.1
libGraphicsMagick++-devel-1.3.25-90.1
libGraphicsMagick++-Q16-12-1.3.25-90.1
GraphicsMagick-devel-1.3.25-90.1
libGraphicsMagickWand-Q16-2-1.3.25-90.1
libGraphicsMagick-Q16-3-debuginfo-1.3.25-90.1
perl-GraphicsMagick-1.3.25-90.1

146707 - SuSE Linux 42.3 openSUSE-SU-2018:1385-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1516, CVE-2017-12597, CVE-2017-12598, CVE-2017-12599, CVE-2017-12600, CVE-2017-12601, CVE-2017-12602, CVE-2017-12603, CVE-2017-12604, CVE-2017-12605, CVE-2017-12606, CVE-2017-12862, CVE-2017-12863, CVE-2017-12864, CVE-2017-14136

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1385-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00089.html

SuSE Linux 42.3
x86_64
python3-opencv-qt5-3.1.0-4.6.1
opencv-qt5-debugsource-3.1.0-4.6.1
python-opencv-qt5-3.1.0-4.6.1
libopencv-qt56_3-3.1.0-4.6.1
libopencv-qt56_3-debuginfo-3.1.0-4.6.1
opencv-debuginfo-3.1.0-4.6.1
libopencv3_1-3.1.0-4.6.1
python-opencv-3.1.0-4.6.1
opencv-qt5-doc-3.1.0-4.6.1
python-opencv-qt5-debuginfo-3.1.0-4.6.1
python-opencv-debuginfo-3.1.0-4.6.1
python3-opencv-debuginfo-3.1.0-4.6.1
opencv-devel-3.1.0-4.6.1
opencv-qt5-3.1.0-4.6.1
opencv-doc-3.1.0-4.6.1
opencv-debugsource-3.1.0-4.6.1
python3-opencv-3.1.0-4.6.1
opencv-qt5-devel-3.1.0-4.6.1
opencv-3.1.0-4.6.1
libopencv3_1-debuginfo-3.1.0-4.6.1
python3-opencv-qt5-debuginfo-3.1.0-4.6.1
opencv-qt5-debuginfo-3.1.0-4.6.1

146708 - SuSE Linux 42.3 openSUSE-SU-2018:1418-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18257, CVE-2018-1000199, CVE-2018-10087, CVE-2018-10124, CVE-2018-1065, CVE-2018-1130, CVE-2018-3639, CVE-2018-5803, CVE-2018-7492, CVE-2018-8781, CVE-2018-8822

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1418-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00110.html

SuSE Linux 42.3
x86_64
kernel-vanilla-devel-4.4.132-53.1
kernel-default-devel-4.4.132-53.1
kernel-vanilla-4.4.132-53.1
kernel-debug-devel-4.4.132-53.1
kselftests-kmp-vanilla-4.4.132-53.1
kernel-debug-devel-debuginfo-4.4.132-53.1
kselftests-kmp-default-4.4.132-53.1
kernel-vanilla-debugsource-4.4.132-53.1
kernel-debug-4.4.132-53.1
kselftests-kmp-default-debuginfo-4.4.132-53.1
kernel-debug-debuginfo-4.4.132-53.1
kernel-vanilla-base-4.4.132-53.1
kernel-debug-base-debuginfo-4.4.132-53.1
kernel-obs-build-debugsource-4.4.132-53.1
kselftests-kmp-debug-4.4.132-53.1
kernel-default-base-4.4.132-53.1
kernel-debug-base-4.4.132-53.1
kernel-vanilla-debuginfo-4.4.132-53.1
kernel-vanilla-base-debuginfo-4.4.132-53.1
kernel-obs-build-4.4.132-53.1
kselftests-kmp-debug-debuginfo-4.4.132-53.1
kernel-default-debuginfo-4.4.132-53.1
kernel-syms-4.4.132-53.1
kernel-obs-qa-4.4.132-53.1
kernel-default-debugsource-4.4.132-53.1
kselftests-kmp-vanilla-debuginfo-4.4.132-53.1
kernel-default-base-debuginfo-4.4.132-53.1
kernel-default-4.4.132-53.1
kernel-debug-debugsource-4.4.132-53.1

noarch
kernel-source-4.4.132-53.1
kernel-docs-4.4.132-53.1
kernel-macros-4.4.132-53.1
kernel-docs-pdf-4.4.132-53.1
kernel-devel-4.4.132-53.1
kernel-docs-html-4.4.132-53.1
kernel-source-vanilla-4.4.132-53.1

146709 - SuSE Linux 42.3 openSUSE-SU-2018:1384-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1046

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1384-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00088.html

SuSE Linux 42.3
x86_64
pdns-backend-mydns-debuginfo-4.0.3-12.1
pdns-backend-geoip-debuginfo-4.0.3-12.1
pdns-debugsource-4.0.3-12.1
pdns-backend-godbc-debuginfo-4.0.3-12.1
pdns-backend-ldap-debuginfo-4.0.3-12.1
pdns-4.0.3-12.1
pdns-backend-remote-4.0.3-12.1
pdns-backend-sqlite3-debuginfo-4.0.3-12.1
pdns-backend-geoip-4.0.3-12.1
pdns-backend-mydns-4.0.3-12.1
pdns-backend-postgresql-4.0.3-12.1
pdns-backend-mysql-4.0.3-12.1
pdns-backend-lua-4.0.3-12.1
pdns-debuginfo-4.0.3-12.1
pdns-backend-postgresql-debuginfo-4.0.3-12.1
pdns-backend-ldap-4.0.3-12.1
pdns-backend-godbc-4.0.3-12.1
pdns-backend-remote-debuginfo-4.0.3-12.1
pdns-backend-sqlite3-4.0.3-12.1
pdns-backend-mysql-debuginfo-4.0.3-12.1
pdns-backend-lua-debuginfo-4.0.3-12.1

146711 - SuSE SLES 11 SP4 SUSE-SU-2018:1449-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10788, CVE-2017-10789

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1449-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004092.html

SuSE SLES 11 SP4
i586
perl-DBD-mysql-4.008-10.5.1

x86_64
perl-DBD-mysql-4.008-10.5.1

146712 - SuSE Linux 15.0 openSUSE-SU-2018:1442-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1046

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1442-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00131.html

SuSE Linux 15.0
x86_64
pdns-debugsource-4.1.2-lp150.3.3.1
pdns-backend-lua-4.1.2-lp150.3.3.1
pdns-backend-mysql-4.1.2-lp150.3.3.1
pdns-backend-geoip-debuginfo-4.1.2-lp150.3.3.1
pdns-backend-geoip-4.1.2-lp150.3.3.1
pdns-4.1.2-lp150.3.3.1
pdns-debuginfo-4.1.2-lp150.3.3.1
pdns-backend-remote-4.1.2-lp150.3.3.1
pdns-backend-mydns-debuginfo-4.1.2-lp150.3.3.1
pdns-backend-godbc-debuginfo-4.1.2-lp150.3.3.1
pdns-backend-postgresql-4.1.2-lp150.3.3.1
pdns-backend-ldap-debuginfo-4.1.2-lp150.3.3.1
pdns-backend-remote-debuginfo-4.1.2-lp150.3.3.1
pdns-backend-sqlite3-4.1.2-lp150.3.3.1
pdns-backend-mysql-debuginfo-4.1.2-lp150.3.3.1
pdns-backend-mydns-4.1.2-lp150.3.3.1
pdns-backend-ldap-4.1.2-lp150.3.3.1
pdns-backend-godbc-4.1.2-lp150.3.3.1
pdns-backend-sqlite3-debuginfo-4.1.2-lp150.3.3.1
pdns-backend-postgresql-debuginfo-4.1.2-lp150.3.3.1
pdns-backend-lua-debuginfo-4.1.2-lp150.3.3.1

146713 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1401-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8146, CVE-2014-8147, CVE-2016-6293, CVE-2017-14952, CVE-2017-15422, CVE-2017-17484, CVE-2017-7867, CVE-2017-7868

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1401-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004085.html

SuSE SLED 12 SP3
x86_64
libicu52_1-52.1-8.7.1
libicu52_1-data-52.1-8.7.1
icu-52.1-8.7.1
libicu52_1-debuginfo-32bit-52.1-8.7.1
icu-debuginfo-52.1-8.7.1
libicu52_1-32bit-52.1-8.7.1
icu-debugsource-52.1-8.7.1
libicu52_1-debuginfo-52.1-8.7.1

SuSE SLES 12 SP3
x86_64
libicu52_1-52.1-8.7.1
libicu52_1-data-52.1-8.7.1
libicu-doc-52.1-8.7.1
libicu52_1-debuginfo-52.1-8.7.1
icu-debuginfo-52.1-8.7.1
libicu52_1-32bit-52.1-8.7.1
icu-debugsource-52.1-8.7.1
libicu52_1-debuginfo-32bit-52.1-8.7.1

146714 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1373-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-0494

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1373-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004075.html

SuSE SLED 12 SP3
x86_64
wget-debugsource-1.14-21.7.1
wget-debuginfo-1.14-21.7.1
wget-1.14-21.7.1

SuSE SLES 12 SP3
x86_64
wget-debugsource-1.14-21.7.1
wget-debuginfo-1.14-21.7.1
wget-1.14-21.7.1

146715 - SuSE Linux 15.0, 42.3 openSUSE-SU-2018:1393-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17688, CVE-2017-17689

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1393-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00091.html

SuSE Linux 15.0
x86_64
enigmail-2.0.5-lp150.2.6.1

SuSE Linux 42.3
x86_64
enigmail-2.0.5-15.1

i586
enigmail-2.0.5-15.1

146717 - SuSE Linux 15.0 openSUSE-SU-2018:1420-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1420-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00112.html

SuSE Linux 15.0
x86_64
kernel-kvmsmall-debugsource-4.12.14-lp150.12.4.1
kernel-obs-qa-4.12.14-lp150.12.4.1
kernel-default-4.12.14-lp150.12.4.1
kernel-debug-base-debuginfo-4.12.14-lp150.12.4.1
kernel-default-debugsource-4.12.14-lp150.12.4.1
kernel-kvmsmall-devel-4.12.14-lp150.12.4.1
kernel-obs-build-4.12.14-lp150.12.4.1
kernel-kvmsmall-devel-debuginfo-4.12.14-lp150.12.4.1
kernel-default-base-4.12.14-lp150.12.4.1
kernel-default-debuginfo-4.12.14-lp150.12.4.1
kernel-debug-4.12.14-lp150.12.4.1
kernel-kvmsmall-debuginfo-4.12.14-lp150.12.4.1
kernel-debug-devel-debuginfo-4.12.14-lp150.12.4.1
kernel-kvmsmall-base-debuginfo-4.12.14-lp150.12.4.1
kernel-default-devel-4.12.14-lp150.12.4.1
kernel-debug-debugsource-4.12.14-lp150.12.4.1
kernel-default-devel-debuginfo-4.12.14-lp150.12.4.1
kernel-debug-debuginfo-4.12.14-lp150.12.4.1
kernel-obs-build-debugsource-4.12.14-lp150.12.4.1
kernel-debug-devel-4.12.14-lp150.12.4.1
kernel-kvmsmall-4.12.14-lp150.12.4.1
kernel-debug-base-4.12.14-lp150.12.4.1
kernel-syms-4.12.14-lp150.12.4.1
kernel-default-base-debuginfo-4.12.14-lp150.12.4.1
kernel-kvmsmall-base-4.12.14-lp150.12.4.1

noarch
kernel-docs-4.12.14-lp150.12.4.1
kernel-devel-4.12.14-lp150.12.4.1

kernel-macros-4.12.14-lp150.12.4.1
kernel-docs-html-4.12.14-lp150.12.4.1
kernel-source-vanilla-4.12.14-lp150.12.4.1
kernel-source-4.12.14-lp150.12.4.1

146721 - SuSE Linux 42.3 openSUSE-SU-2018:1463-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10788, CVE-2017-10789

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1463-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00138.html

SuSE Linux 42.3
x86_64
perl-DBD-mysql-debuginfo-4.021-18.3.1
perl-DBD-mysql-debugsource-4.021-18.3.1
perl-DBD-mysql-4.021-18.3.1

146722 - SuSE Linux 42.3 openSUSE-SU-2018:1422-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8146, CVE-2014-8147, CVE-2016-6293, CVE-2017-14952, CVE-2017-15422, CVE-2017-17484, CVE-2017-7867, CVE-2017-7868

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1422-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00114.html

SuSE Linux 42.3
x86_64
libicu-devel-52.1-18.1
libicu-devel-32bit-52.1-18.1
libicu52_1-debuginfo-32bit-52.1-18.1
icu-debuginfo-52.1-18.1
icu-debugsource-52.1-18.1
libicu-doc-52.1-18.1
libicu52_1-debuginfo-52.1-18.1
icu-52.1-18.1
libicu52_1-data-52.1-18.1
libicu52_1-52.1-18.1

libicu52_1-32bit-52.1-18.1
icu-data-52.1-18.1

i586
libicu-devel-52.1-18.1
icu-debuginfo-52.1-18.1
icu-debugsource-52.1-18.1
libicu-doc-52.1-18.1
libicu52_1-debuginfo-52.1-18.1
icu-52.1-18.1
libicu52_1-data-52.1-18.1
libicu52_1-52.1-18.1
icu-data-52.1-18.1

146725 - SuSE Linux 42.3 openSUSE-SU-2018:1415-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000158, CVE-2018-1000030

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1415-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00108.html

SuSE Linux 42.3
i586
python-curses-debuginfo-2.7.13-27.3.1
python-debugsource-2.7.13-27.3.1
python-tk-debuginfo-2.7.13-27.3.1
python-gdbm-2.7.13-27.3.1
python-devel-2.7.13-27.3.1
python-gdbm-debuginfo-2.7.13-27.3.1
libpython2_7-1_0-2.7.13-27.3.1
python-idle-2.7.13-27.3.1
python-base-debuginfo-2.7.13-27.3.1
python-xml-debuginfo-2.7.13-27.3.1
python-curses-2.7.13-27.3.1
libpython2_7-1_0-debuginfo-2.7.13-27.3.1
python-xml-2.7.13-27.3.1
python-demo-2.7.13-27.3.1
python-base-2.7.13-27.3.1
python-tk-2.7.13-27.3.1
python-debuginfo-2.7.13-27.3.1
python-base-debugsource-2.7.13-27.3.1
python-2.7.13-27.3.1

noarch
python-doc-pdf-2.7.13-27.3.1
python-doc-2.7.13-27.3.1

x86_64
python-curses-debuginfo-2.7.13-27.3.1

python-debugsource-2.7.13-27.3.1
python-tk-debuginfo-2.7.13-27.3.1
python-gdbm-2.7.13-27.3.1
libpython2_7-1_0-debuginfo-32bit-2.7.13-27.3.1
python-devel-2.7.13-27.3.1
python-gdbm-debuginfo-2.7.13-27.3.1
libpython2_7-1_0-2.7.13-27.3.1
python-idle-2.7.13-27.3.1
python-base-debuginfo-2.7.13-27.3.1
python-base-32bit-2.7.13-27.3.1
python-32bit-2.7.13-27.3.1
python-base-debuginfo-32bit-2.7.13-27.3.1
libpython2_7-1_0-32bit-2.7.13-27.3.1
python-xml-debuginfo-2.7.13-27.3.1
python-debuginfo-32bit-2.7.13-27.3.1
python-curses-2.7.13-27.3.1
libpython2_7-1_0-debuginfo-2.7.13-27.3.1
python-xml-2.7.13-27.3.1
python-demo-2.7.13-27.3.1
python-base-2.7.13-27.3.1
python-tk-2.7.13-27.3.1
python-debuginfo-2.7.13-27.3.1
python-base-debugsource-2.7.13-27.3.1
python-2.7.13-27.3.1

146726 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1378-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1378-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004080.html

SuSE SLED 12 SP3
x86_64
qemu-x86-2.9.1-6.16.1
qemu-block-curl-debuginfo-2.9.1-6.16.1
qemu-2.9.1-6.16.1
qemu-tools-2.9.1-6.16.1
qemu-kvm-2.9.1-6.16.1
qemu-tools-debuginfo-2.9.1-6.16.1
qemu-debugsource-2.9.1-6.16.1
qemu-block-curl-2.9.1-6.16.1

noarch
qemu-ipxe-1.0.0-6.16.1
qemu-sgabios-8-6.16.1
qemu-vgabios-1.10.2-6.16.1
qemu-seabios-1.10.2-6.16.1

SuSE SLES 12 SP3
noarch
qemu-ipxe-1.0.0-6.16.1
qemu-sgabios-8-6.16.1
qemu-vgabios-1.10.2-6.16.1
qemu-seabios-1.10.2-6.16.1

x86_64
qemu-guest-agent-2.9.1-6.16.1
qemu-2.9.1-6.16.1
qemu-block-curl-debuginfo-2.9.1-6.16.1
qemu-block-ssh-2.9.1-6.16.1
qemu-block-ssh-debuginfo-2.9.1-6.16.1
qemu-x86-2.9.1-6.16.1
qemu-tools-debuginfo-2.9.1-6.16.1
qemu-x86-debuginfo-2.9.1-6.16.1
qemu-guest-agent-debuginfo-2.9.1-6.16.1
qemu-lang-2.9.1-6.16.1
qemu-tools-2.9.1-6.16.1
qemu-debugsource-2.9.1-6.16.1
qemu-block-curl-2.9.1-6.16.1
qemu-kvm-2.9.1-6.16.1
qemu-block-iscsi-2.9.1-6.16.1
qemu-block-iscsi-debuginfo-2.9.1-6.16.1
qemu-block-rbd-debuginfo-2.9.1-6.16.1
qemu-block-rbd-2.9.1-6.16.1

146727 - SuSE Linux 42.3 openSUSE-SU-2018:1380-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1380-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00085.html

SuSE Linux 42.3
i586
qemu-linux-user-2.9.1-44.1
qemu-linux-user-debuginfo-2.9.1-44.1
qemu-linux-user-debugsource-2.9.1-44.1

noarch
qemu-seabios-1.10.2-44.1
qemu-ipxe-1.0.0-44.1
qemu-sgabios-8-44.1
qemu-vgabios-1.10.2-44.1

x86_64
qemu-s390-debuginfo-2.9.1-44.1
qemu-ppc-2.9.1-44.1

qemu-block-ssh-2.9.1-44.1
qemu-2.9.1-44.1
qemu-block-iscsi-debuginfo-2.9.1-44.1
qemu-arm-debuginfo-2.9.1-44.1
qemu-lang-2.9.1-44.1
qemu-block-dmg-debuginfo-2.9.1-44.1
qemu-block-ssh-debuginfo-2.9.1-44.1
qemu-debugsource-2.9.1-44.1
qemu-x86-2.9.1-44.1
qemu-kvm-2.9.1-44.1
qemu-linux-user-2.9.1-44.1
qemu-block-rbd-debuginfo-2.9.1-44.1
qemu-linux-user-debuginfo-2.9.1-44.1
qemu-block-dmg-2.9.1-44.1
qemu-extra-debuginfo-2.9.1-44.1
qemu-tools-debuginfo-2.9.1-44.1
qemu-arm-2.9.1-44.1
qemu-guest-agent-2.9.1-44.1
qemu-x86-debuginfo-2.9.1-44.1
qemu-testsuite-2.9.1-44.1
qemu-guest-agent-debuginfo-2.9.1-44.1
qemu-block-curl-debuginfo-2.9.1-44.1
qemu-block-rbd-2.9.1-44.1
qemu-block-curl-2.9.1-44.1
qemu-ppc-debuginfo-2.9.1-44.1
qemu-tools-2.9.1-44.1
qemu-s390-2.9.1-44.1
qemu-extra-2.9.1-44.1
qemu-ksm-2.9.1-44.1
qemu-linux-user-debugsource-2.9.1-44.1
qemu-block-iscsi-2.9.1-44.1

146728 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1398-1 Update Is Not Installed

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

Risk Level: High

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

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1398-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004084.html

SuSE SLED 12 SP3
x86_64
bash-4.3-83.10.1
libreadline6-debuginfo-6.3-83.10.1
bash-debugsource-4.3-83.10.1
libreadline6-32bit-6.3-83.10.1
libreadline6-debuginfo-32bit-6.3-83.10.1
bash-debuginfo-4.3-83.10.1
libreadline6-6.3-83.10.1

noarch
readline-doc-6.3-83.10.1
bash-doc-4.3-83.10.1
bash-lang-4.3-83.10.1

SuSE SLES 12 SP3
noarch
readline-doc-6.3-83.10.1
bash-doc-4.3-83.10.1

x86_64
bash-4.3-83.10.1
libreadline6-debuginfo-6.3-83.10.1
bash-debugsource-4.3-83.10.1
libreadline6-32bit-6.3-83.10.1
libreadline6-debuginfo-32bit-6.3-83.10.1
bash-debuginfo-4.3-83.10.1
libreadline6-6.3-83.10.1

146729 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1456-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10981, CVE-2018-10982, CVE-2018-3639

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1456-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004096.html

SuSE SLED 12 SP3
x86_64
xen-libs-4.9.2_06-3.32.1
xen-libs-debuginfo-32bit-4.9.2_06-3.32.1
xen-4.9.2_06-3.32.1
xen-libs-debuginfo-4.9.2_06-3.32.1
xen-debugsource-4.9.2_06-3.32.1
xen-libs-32bit-4.9.2_06-3.32.1

SuSE SLES 12 SP3
x86_64
xen-tools-debuginfo-4.9.2_06-3.32.1
xen-libs-4.9.2_06-3.32.1
xen-debugsource-4.9.2_06-3.32.1
xen-tools-domU-4.9.2_06-3.32.1
xen-4.9.2_06-3.32.1
xen-doc-html-4.9.2_06-3.32.1
xen-libs-debuginfo-4.9.2_06-3.32.1
xen-libs-32bit-4.9.2_06-3.32.1
xen-tools-domU-debuginfo-4.9.2_06-3.32.1
xen-tools-4.9.2_06-3.32.1
xen-libs-debuginfo-32bit-4.9.2_06-3.32.1

146733 - SuSE SLES 12 SP3 SUSE-SU-2018:1450-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10788, CVE-2017-10789

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1450-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004093.html

SuSE SLES 12 SP3
x86_64
perl-DBD-mysql-4.021-12.5.2
perl-DBD-mysql-debuginfo-4.021-12.5.2
perl-DBD-mysql-debugsource-4.021-12.5.2

146734 - SuSE Linux 42.3 openSUSE-SU-2018:1383-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-0494

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1383-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00087.html

SuSE Linux 42.3
x86_64
wget-debugsource-1.14-15.1
wget-debuginfo-1.14-15.1
wget-1.14-15.1

i586
wget-debugsource-1.14-15.1
wget-debuginfo-1.14-15.1
wget-1.14-15.1

146735 - SuSE Linux 15.0 openSUSE-SU-2018:1421-1 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:
openSUSE-SU-2018:1421-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00113.html

SuSE Linux 15.0
x86_64
libGraphicsMagick-Q16-3-1.3.29-lp150.3.3.1
GraphicsMagick-1.3.29-lp150.3.3.1
perl-GraphicsMagick-debuginfo-1.3.29-lp150.3.3.1
GraphicsMagick-debugsource-1.3.29-lp150.3.3.1
libGraphicsMagick++-devel-1.3.29-lp150.3.3.1
libGraphicsMagick++-Q16-12-1.3.29-lp150.3.3.1
libGraphicsMagick3-config-1.3.29-lp150.3.3.1
GraphicsMagick-devel-1.3.29-lp150.3.3.1
libGraphicsMagickWand-Q16-2-1.3.29-lp150.3.3.1
libGraphicsMagick-Q16-3-debuginfo-1.3.29-lp150.3.3.1
libGraphicsMagickWand-Q16-2-debuginfo-1.3.29-lp150.3.3.1
perl-GraphicsMagick-1.3.29-lp150.3.3.1
libGraphicsMagick++-Q16-12-debuginfo-1.3.29-lp150.3.3.1
GraphicsMagick-debuginfo-1.3.29-lp150.3.3.1

146736 - SuSE Linux 15.0, 42.3 openSUSE-SU-2018:1454-1 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:
openSUSE-SU-2018:1454-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00133.html

SuSE Linux 15.0
x86_64
enigmail-2.0.6-lp150.2.9.1

SuSE Linux 42.3
x86_64
enigmail-2.0.6-18.1

i586
enigmail-2.0.6-18.1

146738 - SuSE Linux 42.3 openSUSE-SU-2018:1381-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-1239, CVE-2017-171479, CVE-2017-17479, CVE-2017-17480

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1381-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00086.html

SuSE Linux 42.3
x86_64
libopenjp2-7-debuginfo-2.1.0-22.1
libopenjp2-7-32bit-2.1.0-22.1
openjpeg2-debuginfo-2.1.0-22.1
libopenjp2-7-debuginfo-32bit-2.1.0-22.1
openjpeg2-devel-2.1.0-22.1
libopenjp2-7-2.1.0-22.1
openjpeg2-2.1.0-22.1
openjpeg2-debugsource-2.1.0-22.1

i586
libopenjp2-7-debuginfo-2.1.0-22.1
openjpeg2-debuginfo-2.1.0-22.1
openjpeg2-devel-2.1.0-22.1
libopenjp2-7-2.1.0-22.1
openjpeg2-2.1.0-22.1
openjpeg2-debugsource-2.1.0-22.1

146740 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1372-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000158, CVE-2018-1000030

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1372-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004074.html

SuSE SLED 12 SP3
x86_64
python-base-2.7.13-28.3.2
libpython2_7-1_0-debuginfo-2.7.13-28.3.2
libpython2_7-1_0-32bit-2.7.13-28.3.2
python-debuginfo-2.7.13-28.3.2
libpython2_7-1_0-debuginfo-32bit-2.7.13-28.3.2
python-curses-2.7.13-28.3.2

python-tk-2.7.13-28.3.2
python-base-debuginfo-2.7.13-28.3.2
python-debugsource-2.7.13-28.3.2
python-2.7.13-28.3.2
python-base-debuginfo-32bit-2.7.13-28.3.2
python-tk-debuginfo-2.7.13-28.3.2
libpython2_7-1_0-2.7.13-28.3.2
python-base-debugsource-2.7.13-28.3.2
python-curses-debuginfo-2.7.13-28.3.2
python-xml-2.7.13-28.3.2
python-xml-debuginfo-2.7.13-28.3.2
python-devel-2.7.13-28.3.2

SuSE SLES 12 SP3
noarch
python-doc-pdf-2.7.13-28.3.3
python-doc-2.7.13-28.3.3

x86_64
python-demo-2.7.13-28.3.2
python-debugsource-2.7.13-28.3.2
libpython2_7-1_0-debuginfo-2.7.13-28.3.2
python-debuginfo-2.7.13-28.3.2
libpython2_7-1_0-debuginfo-32bit-2.7.13-28.3.2
python-base-debuginfo-32bit-2.7.13-28.3.2
python-curses-2.7.13-28.3.2
python-base-2.7.13-28.3.2
libpython2_7-1_0-32bit-2.7.13-28.3.2
python-tk-2.7.13-28.3.2
python-base-debuginfo-2.7.13-28.3.2
python-gdbm-2.7.13-28.3.2
python-32bit-2.7.13-28.3.2
python-gdbm-debuginfo-2.7.13-28.3.2
python-base-32bit-2.7.13-28.3.2
python-2.7.13-28.3.2
python-xml-debuginfo-2.7.13-28.3.2
python-idle-2.7.13-28.3.2
python-tk-debuginfo-2.7.13-28.3.2
libpython2_7-1_0-2.7.13-28.3.2
python-base-debugsource-2.7.13-28.3.2
python-curses-debuginfo-2.7.13-28.3.2
python-xml-2.7.13-28.3.2
python-debuginfo-32bit-2.7.13-28.3.2

160403 - CentOS 6 CESA-2018-1669 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
CESA-2018-1669

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022845.html

CentOS 6
x86_64
libvirt-lock-sanlock-0.10.2-62.el6_9.2
libvirt-devel-0.10.2-62.el6_9.2
libvirt-client-0.10.2-62.el6_9.2
libvirt-0.10.2-62.el6_9.2
libvirt-python-0.10.2-62.el6_9.2

i686
libvirt-devel-0.10.2-62.el6_9.2
libvirt-client-0.10.2-62.el6_9.2
libvirt-0.10.2-62.el6_9.2
libvirt-python-0.10.2-62.el6_9.2

160404 - CentOS 7 CESA-2018-1725 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5159, CVE-2018-5161, CVE-2018-5162, CVE-2018-5168, CVE-2018-5170, CVE-2018-5178, CVE-2018-5183, CVE-2018-5184, CVE-2018-5185

Description

The scan detected that the host is missing the following update:
CESA-2018-1725

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022848.html

CentOS 7
x86_64
thunderbird-52.8.0-1.el7.centos

160405 - CentOS 6 CESA-2018-1726 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5159, CVE-2018-5161, CVE-2018-5162, CVE-2018-5168, CVE-2018-5170, CVE-2018-5178, CVE-2018-5183, CVE-2018-5184, CVE-2018-5185

Description

The scan detected that the host is missing the following update:
CESA-2018-1726

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022846.html

CentOS 6
x86_64

thunderbird-52.8.0-2.el6.centos

i686
thunderbird-52.8.0-2.el6.centos

160406 - CentOS 7 CESA-2018-1700 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1124, CVE-2018-1126

Description

The scan detected that the host is missing the following update:
CESA-2018-1700

Observation

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

http://lists.centos.org/pipermail/centos-announce/2018-May/022847.html

CentOS 7
x86_64
procps-ng-i18n-3.3.10-17.el7_5.2
procps-ng-3.3.10-17.el7_5.2
procps-ng-devel-3.3.10-17.el7_5.2

i686
procps-ng-devel-3.3.10-17.el7_5.2
procps-ng-3.3.10-17.el7_5.2

163630 - Oracle Enterprise Linux ELSA-2018-1726 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5159, CVE-2018-5161, CVE-2018-5162, CVE-2018-5168, CVE-2018-5170, CVE-2018-5178, CVE-2018-5183, CVE-2018-5184, CVE-2018-5185

Description

The scan detected that the host is missing the following update:
ELSA-2018-1726

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007765.html

OEL6
x86_64
thunderbird-52.8.0-2.0.1.el6_9

i386
thunderbird-52.8.0-2.0.1.el6_9

163632 - Oracle Enterprise Linux ELSA-2018-1725 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5159, CVE-2018-5161, CVE-2018-5162, CVE-2018-5168, CVE-2018-5170, CVE-2018-5178, CVE-2018-5183, CVE-2018-5184, CVE-2018-5185

Description

The scan detected that the host is missing the following update:
ELSA-2018-1725

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007764.html

OEL7
x86_64
thunderbird-52.8.0-1.0.1.el7_5

163633 - Oracle Enterprise Linux ELSA-2018-1700 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1124, CVE-2018-1126

Description

The scan detected that the host is missing the following update:
ELSA-2018-1700

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007762.html

OEL7
x86_64
procps-ng-i18n-3.3.10-17.el7_5.2
procps-ng-3.3.10-17.el7_5.2
procps-ng-devel-3.3.10-17.el7_5.2

170976 - Amazon Linux AMI ALAS-2018-1023 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16939, CVE-2018-1000199, CVE-2018-1068, CVE-2018-1087, CVE-2018-1091, CVE-2018-1108, CVE-2018-8897

Description

The scan detected that the host is missing the following update:
ALAS-2018-1023

Observation

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

https://alas.aws.amazon.com/ALAS-2018-1023.html

Amazon Linux AMI
x86_64
kernel-debuginfo-4.14.42-52.37.amzn1
kernel-debuginfo-common-x86_64-4.14.42-52.37.amzn1
kernel-tools-4.14.42-52.37.amzn1
perf-debuginfo-4.14.42-52.37.amzn1
kernel-tools-devel-4.14.42-52.37.amzn1
kernel-4.14.42-52.37.amzn1
kernel-tools-debuginfo-4.14.42-52.37.amzn1
kernel-headers-4.14.42-52.37.amzn1
perf-4.14.42-52.37.amzn1
kernel-devel-4.14.42-52.37.amzn1

i686
kernel-debuginfo-common-i686-4.14.42-52.37.amzn1
kernel-debuginfo-4.14.42-52.37.amzn1
kernel-tools-4.14.42-52.37.amzn1
kernel-devel-4.14.42-52.37.amzn1
kernel-tools-devel-4.14.42-52.37.amzn1
kernel-4.14.42-52.37.amzn1
kernel-tools-debuginfo-4.14.42-52.37.amzn1
perf-debuginfo-4.14.42-52.37.amzn1
perf-4.14.42-52.37.amzn1
kernel-headers-4.14.42-52.37.amzn1

178634 - Gentoo Linux GLSA-201805-13 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201805-13

Observation

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

https://security.gentoo.org/glsa/201805-13

Affected packages:
dev-vcs/git < 2.16.4

186233 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3662-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-6249, CVE-2018-6253

Description

The scan detected that the host is missing the following update:
USN-3662-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-May/004417.html

Ubuntu 16.04

nvidia-384_384.130-0ubuntu0.16.04.1

Ubuntu 14.04

nvidia-384_384.130-0ubuntu0.14.04.1

Ubuntu 17.10

nvidia-384_384.130-0ubuntu0.17.10.1

193747 - Fedora Linux 27 FEDORA-2018-9d0e4e40b5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-12193, CVE-2017-15115, CVE-2017-16532, CVE-2017-16538, CVE-2017-16644, CVE-2017-16647, CVE-2017-16649, CVE-2017-16650, CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-17558, CVE-2017-17712, CVE-2017-17741, CVE-2017-17852, CVE-2017-17853, CVE-2017-17854, CVE-2017-17855, CVE-2017-17856, CVE-2017-17857, CVE-2017-17862, CVE-2017-17863, CVE-2017-17864, CVE-2017-18232, CVE-2017-8824, CVE-2018-1000004, CVE-2018-1000026, CVE-2018-10021, CVE-2018-10322, CVE-2018-10323, CVE-2018-1065, CVE-2018-10840, CVE-2018-1108, CVE-2018-1120, CVE-2018-3639, CVE-2018-5332, CVE-2018-5333, CVE-2018-5344, CVE-2018-5750, CVE-2018-5803, CVE-2018-7757, CVE-2018-7995, CVE-2018-8043

Description

The scan detected that the host is missing the following update:
FEDORA-2018-9d0e4e40b5

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/2018/5/?count=200&page=1

Fedora Core 27

kernel-4.16.12-200.fc27

193749 - Fedora Linux 27 FEDORA-2018-9dc7338487 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000254, CVE-2017-1000257, CVE-2017-8816, CVE-2017-8817, CVE-2018-1000005, CVE-2018-1000007, CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2018-1000300, CVE-2018-1000301

Description

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

FEDORA-2018-9dc7338487

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/2018/5/?count=200&page=2

Fedora Core 27

curl-7.55.1-11.fc27

193753 - Fedora Linux 26 FEDORA-2018-7be77249d4 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17742, CVE-2018-6914, CVE-2018-8777, CVE-2018-8778, CVE-2018-8779, CVE-2018-8780

Description

The scan detected that the host is missing the following update:
FEDORA-2018-7be77249d4

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/2018/5/?count=200&page=1

Fedora Core 26

ruby-2.4.4-88.fc26

193754 - Fedora Linux 27 FEDORA-2018-93c2e74446 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000405, CVE-2017-12193, CVE-2017-15115, CVE-2017-16532, CVE-2017-16538, CVE-2017-16644, CVE-2017-16647, CVE-2017-16649, CVE-2017-16650, CVE-2017-17448, CVE-2017-17449, CVE-2017-17450, CVE-2017-17558, CVE-2017-17712, CVE-2017-17741, CVE-2017-17852, CVE-2017-17853, CVE-2017-17854, CVE-2017-17855, CVE-2017-17856, CVE-2017-17857, CVE-2017-17862, CVE-2017-17863, CVE-2017-17864, CVE-2017-18232, CVE-2017-8824, CVE-2018-1000004, CVE-2018-1000026, CVE-2018-10021, CVE-2018-10322, CVE-2018-10323, CVE-2018-1065, CVE-2018-1108, CVE-2018-1120, CVE-2018-3639, CVE-2018-5332, CVE-2018-5333, CVE-2018-5344, CVE-2018-5750, CVE-2018-5803, CVE-2018-7757, CVE-2018-7995, CVE-2018-8043

Description

The scan detected that the host is missing the following update:
FEDORA-2018-93c2e74446

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/2018/5/?count=200&page=2

Fedora Core 27

kernel-4.16.11-200.fc27

23611 - (K25573437) F5 BIG-IP TMM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2018-5517

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the Traffic Management Microkernel (TMM). Successful exploitation could allow an attacker to cause a denial of service condition in the target system.

23615 - Apache Tomcat Vulnerability Prior To 9.0.5

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

Risk Level: Medium

CVE: CVE-2018-8014

Description

A vulnerability is present in some versions of Apache Tomcat.

Observation

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

A vulnerability is present in some versions of Apache Tomcat. The flaw lies in default settings for the CORS filter. Successful exploitation could allow an attacker to bypass CORS protocol's security design and cause many misconfiguration security problems.

23618 - (SB10234) McAfee ePolicy Orchestrator Multiple Java Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2018-2783, CVE-2018-2794, CVE-2018-2795, CVE-2018-2796, CVE-2018-2797, CVE-2018-2799, CVE-2018-2815

Description

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator.

Observation

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

Multiple vulnerabilities are present in some versions of McAfee ePolicy Orchestrator. The flaws are related with the Java component. Successful exploitation could allow an attacker to retrieve sensitive data, cause a denial of service condition or do unauthorized modifications on the target system.

23620 - Cisco Adaptive Security Appliance Application Layer Protocol Inspection Denial of Service Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-0240

Description

Multiple vulnerabilities are present in some versions of Cisco Adaptive Security Appliance (ASA).

Observation

Cisco Adaptive Security Appliance is a firewall device.

Multiple vulnerabilities are present in some versions of Cisco Adaptive Security Appliance (ASA). The flaws lie in Application Layer Protocol. Successful exploitation could allow an unauthenticated remote attacker to cause denial of service condition.

23633 - IBM DB2 Db2convert Tool Buffer Overflow Vulnerability (swg22016140)

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

Risk Level: Medium

CVE: CVE-2018-1515

Description

A privilege escalation vulnerability is present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

A privilege escalation vulnerability is present in some versions of IBM DB2. The flaw lies in db2convert component. Successful exploitation could allow a local attacker to gain elevated privileges under specific conditions. The exploit requires the attacker to have valid credentials to the vulnerable system.

23634 - IBM DB2 Db2convert Tool Buffer Overflow Vulnerability (swg22016140)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-1515

Description

A privilege escalation vulnerability is present in some versions of IBM DB2.

Observation

IBM DB2 is a popular relational database management server.

A privilege escalation vulnerability is present in some versions of IBM DB2. The flaw lies in db2convert component. Successful exploitation could allow a local attacker to gain elevated privileges under specific conditions. The exploit requires the attacker to have valid credentials to the vulnerable system.

23636 - (K05263202) F5 BIG-IP IPsec tunnel endpoint Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2017-6156

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in IPsec component. Successful exploitation could allow remote attackers to cause a denial of service.

23638 - Joomla Media Manager XSS Vulnerability (20180509)

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

Risk Level: Medium

CVE: CVE-2018-6378

Description

An XSS vulnerability is present in some versions of Joomla!.

Observation

Joomla! is an open source content management system.

An XSS vulnerability is present in some versions of Joomla!. The flaw is due to an inadequate filtering of file and folder names in the media manager. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

23639 - Joomla Redirect Method XSS Vulnerability (20180508)

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

Risk Level: Medium

CVE: CVE-2018-11328

Description

A XSS vulnerability is present in some versions of Joomla!.

Observation

Joomla! is an open source content management system.

A XSS vulnerability is present in some versions of Joomla!. The flaw is due to an inadequate escaping of username and password included in URI used by redirect. Successful exploitation could allow an attacker to execute arbitrary code on the target system.

132459 - Oracle VM OVMSA-2018-0224 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-17563, CVE-2017-17564, CVE-2017-17565, CVE-2017-17566, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0224

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-May/000859.html

OVM3.3
x86_64
xen-tools-4.3.0-55.el6.186.143
xen-4.3.0-55.el6.186.143

146718 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1441-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-4233, CVE-2013-4234

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1441-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004089.html

SuSE SLED 12 SP3
x86_64
libmodplug-debugsource-0.8.9.0+git20170610.f6dd59a-15.4.1
libmodplug1-0.8.9.0+git20170610.f6dd59a-15.4.1
libmodplug1-debuginfo-0.8.9.0+git20170610.f6dd59a-15.4.1

SuSE SLES 12 SP3
x86_64
libmodplug-debugsource-0.8.9.0+git20170610.f6dd59a-15.4.1
libmodplug1-0.8.9.0+git20170610.f6dd59a-15.4.1
libmodplug1-debuginfo-0.8.9.0+git20170610.f6dd59a-15.4.1

146724 - SuSE Linux 42.3 openSUSE-SU-2018:1438-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000450, CVE-2017-17760, CVE-2017-18009, CVE-2018-5268, CVE-2018-5269

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1438-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00128.html

SuSE Linux 42.3
x86_64
opencv-3.1.0-4.11.1
opencv-doc-3.1.0-4.11.1
opencv-qt5-debuginfo-3.1.0-4.11.1
opencv-qt5-devel-3.1.0-4.11.1
python-opencv-debuginfo-3.1.0-4.11.1

libopencv-qt56_3-debuginfo-3.1.0-4.11.1
opencv-debuginfo-3.1.0-4.11.1
python-opencv-qt5-3.1.0-4.11.1
python-opencv-qt5-debuginfo-3.1.0-4.11.1
libopencv3_1-debuginfo-3.1.0-4.11.1
python3-opencv-qt5-debuginfo-3.1.0-4.11.1
libopencv-qt56_3-3.1.0-4.11.1
python-opencv-3.1.0-4.11.1
python3-opencv-debuginfo-3.1.0-4.11.1
opencv-qt5-debugsource-3.1.0-4.11.1
opencv-qt5-3.1.0-4.11.1
libopencv3_1-3.1.0-4.11.1
opencv-debugsource-3.1.0-4.11.1
python3-opencv-3.1.0-4.11.1
python3-opencv-qt5-3.1.0-4.11.1
opencv-devel-3.1.0-4.11.1
opencv-qt5-doc-3.1.0-4.11.1

146731 - SuSE SLES 11 SP4 SUSE-SU-2018:1369-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9601, CVE-2018-10194

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1369-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004073.html

SuSE SLES 11 SP4
i586
ghostscript-omni-8.62-32.47.10.1
ghostscript-library-8.62-32.47.10.1
ghostscript-fonts-rus-8.62-32.47.10.1
ghostscript-fonts-std-8.62-32.47.10.1
ghostscript-fonts-other-8.62-32.47.10.1
libgimpprint-4.2.7-32.47.10.1
ghostscript-x11-8.62-32.47.10.1

x86_64
ghostscript-omni-8.62-32.47.10.1
ghostscript-library-8.62-32.47.10.1
ghostscript-fonts-rus-8.62-32.47.10.1
ghostscript-fonts-std-8.62-32.47.10.1
ghostscript-fonts-other-8.62-32.47.10.1
libgimpprint-4.2.7-32.47.10.1
ghostscript-x11-8.62-32.47.10.1

146737 - SuSE SLES 11 SP4 SUSE-SU-2018:1447-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1417, CVE-2018-2783, CVE-2018-2790, CVE-2018-2794, CVE-2018-2795, CVE-2018-2796, CVE-2018-2797, CVE-2018-2798, CVE-2018-2799, CVE-2018-2800, CVE-2018-2814

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1447-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004090.html

SuSE SLES 11 SP4
i586
java-1_7_1-ibm-1.7.1_sr4.25-26.26.1
java-1_7_1-ibm-jdbc-1.7.1_sr4.25-26.26.1
java-1_7_1-ibm-plugin-1.7.1_sr4.25-26.26.1
java-1_7_1-ibm-alsa-1.7.1_sr4.25-26.26.1

x86_64
java-1_7_1-ibm-1.7.1_sr4.25-26.26.1
java-1_7_1-ibm-jdbc-1.7.1_sr4.25-26.26.1
java-1_7_1-ibm-plugin-1.7.1_sr4.25-26.26.1
java-1_7_1-ibm-alsa-1.7.1_sr4.25-26.26.1

170977 - Amazon Linux AMI ALAS-2018-1027 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2755, CVE-2018-2758, CVE-2018-2761, CVE-2018-2766, CVE-2018-2771, CVE-2018-2773, CVE-2018-2781, CVE-2018-2782, CVE-2018-2784, CVE-2018-2787, CVE-2018-2813, CVE-2018-2817, CVE-2018-2818, CVE-2018-2819

Description

The scan detected that the host is missing the following update:
ALAS-2018-1027

Observation

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

https://alas.aws.amazon.com/ALAS-2018-1027.html

Amazon Linux AMI
x86_64
mysql56-common-5.6.40-1.29.amzn1
mysql56-bench-5.6.40-1.29.amzn1
mysql56-server-5.6.40-1.29.amzn1
mysql56-test-5.6.40-1.29.amzn1
mysql56-debuginfo-5.6.40-1.29.amzn1
mysql56-embedded-devel-5.6.40-1.29.amzn1
mysql56-errmsg-5.6.40-1.29.amzn1
mysql56-devel-5.6.40-1.29.amzn1
mysql56-embedded-5.6.40-1.29.amzn1
mysql56-libs-5.6.40-1.29.amzn1
mysql56-5.6.40-1.29.amzn1

i686
mysql56-common-5.6.40-1.29.amzn1
mysql56-errmsg-5.6.40-1.29.amzn1
mysql56-bench-5.6.40-1.29.amzn1
mysql56-test-5.6.40-1.29.amzn1
mysql56-server-5.6.40-1.29.amzn1
mysql56-debuginfo-5.6.40-1.29.amzn1
mysql56-embedded-devel-5.6.40-1.29.amzn1
mysql56-embedded-5.6.40-1.29.amzn1
mysql56-devel-5.6.40-1.29.amzn1
mysql56-libs-5.6.40-1.29.amzn1
mysql56-5.6.40-1.29.amzn1

170981 - Amazon Linux AMI ALAS-2018-1026 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2755, CVE-2018-2758, CVE-2018-2759, CVE-2018-2761, CVE-2018-2762, CVE-2018-2766, CVE-2018-2769, CVE-2018-2771, CVE-2018-2773, CVE-2018-2775, CVE-2018-2776, CVE-2018-2777, CVE-2018-2778, CVE-2018-2779, CVE-2018-2780, CVE-2018-2781, CVE-2018-2782, CVE-2018-2784, CVE-2018-2786, CVE-2018-2787, CVE-2018-2810, CVE-2018-2812, CVE-2018-2813, CVE-2018-2816, CVE-2018-2817, CVE-2018-2818, CVE-2018-2819, CVE-2018-2839, CVE-2018-2846

Description

The scan detected that the host is missing the following update:
ALAS-2018-1026

Observation

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

https://alas.aws.amazon.com/ALAS-2018-1026.html

Amazon Linux AMI
x86_64
mysql57-embedded-devel-5.7.22-2.7.amzn1
mysql57-debuginfo-5.7.22-2.7.amzn1
mysql57-common-5.7.22-2.7.amzn1
mysql57-devel-5.7.22-2.7.amzn1
mysql57-errmsg-5.7.22-2.7.amzn1
mysql57-embedded-5.7.22-2.7.amzn1
mysql57-libs-5.7.22-2.7.amzn1
mysql57-5.7.22-2.7.amzn1
mysql57-test-5.7.22-2.7.amzn1
mysql57-server-5.7.22-2.7.amzn1

i686
mysql57-embedded-devel-5.7.22-2.7.amzn1
mysql57-debuginfo-5.7.22-2.7.amzn1
mysql57-common-5.7.22-2.7.amzn1
mysql57-devel-5.7.22-2.7.amzn1
mysql57-errmsg-5.7.22-2.7.amzn1
mysql57-embedded-5.7.22-2.7.amzn1
mysql57-libs-5.7.22-2.7.amzn1
mysql57-5.7.22-2.7.amzn1
mysql57-test-5.7.22-2.7.amzn1
mysql57-server-5.7.22-2.7.amzn1

193742 - Fedora Linux 27 FEDORA-2018-d6002f761d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10536, CVE-2018-10537, CVE-2018-10538, CVE-2018-10539, CVE-2018-10540, CVE-2018-6767, CVE-2018-7253

Description

The scan detected that the host is missing the following update:
FEDORA-2018-d6002f761d

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/2018/5/?count=200&page=1

Fedora Core 27

wavpack-5.1.0-8.fc27

23527 - (JSA10851) Juniper Junos OS OpenSSL Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-3193, CVE-2016-0701, CVE-2017-3732, CVE-2017-3735, CVE-2017-3736, CVE-2017-3737, CVE-2017-3738

Description

Multiple vulnerabilities are present in some versions of Juniper Junos OS.

Observation

Juniper Junos OS is an operating system used in Juniper devices.

Multiple vulnerabilities are present in some versions of Juniper Junos OS. The flaws lie in the OpenSSL component. Successful exploitation could allow an attacker to obtain sensitive data.

23624 - Apache Tomcat Vulnerability Prior To 8.0.53

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

Risk Level: Medium

CVE: CVE-2018-8014

Description

A vulnerability is present in some versions of Apache Tomcat.

Observation

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

A vulnerability is present in some versions of Apache Tomcat. The flaw lies in default settings for the CORS filter. Successful exploitation could allow an attacker to bypass certain security restrictions.

23625 - (HPESBGN03763) HPE SiteScope Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-8949, CVE-2017-8950, CVE-2017-8951, CVE-2017-8952

Description

Multiple vulnerabilities are present in some versions of HP SiteScope.

Observation

HP SiteScope is an agent-less monitoring software that monitors the availability and performance of IT infrastructures and application components remotely.

Multiple vulnerabilities are present in some versions of HP SiteScope. The flaws lie in multiple components. Successful exploitation could allow an attacker to locally disclose sensitive information and bypass security restrictions or remotely execute arbitrary code.

23627 - (K34035645) F5 BIG-IP Wireshark Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2018-7320, CVE-2018-7321, CVE-2018-7322, CVE-2018-7323, CVE-2018-7324, CVE-2018-7325, CVE-2018-7326, CVE-2018-7327, CVE-2018-7328, CVE-2018-7329, CVE-2018-7330, CVE-2018-7331, CVE-2018-7332, CVE-2018-7333, CVE-2018-7334, CVE-2018-7335, CVE-2018-7336, CVE-2018-7337, CVE-2018-7417, CVE-2018-7418, CVE-2018-7419, CVE-2018-7420, CVE-2018-7421

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 impacts on the target system.

23629 - IBM AIX Speculative Store Bypass Vulnerability (variant4_advisory)

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

Risk Level: Medium

CVE: CVE-2018-3639

Description

A vulnerability is present in some versions of IBM AIX.

Observation

AIX is a Unix-like operating system developed by IBM.

A vulnerability is present in some versions of IBM AIX. The flaw is due to a weakness in microprocessors. Successful exploitation could allow a local attacker to obtain sensitive information.

23642 - Wireshark Multiple Vulnerabilities Prior To 2.2.15

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

Risk Level: Medium

CVE: CVE-2018-11356, CVE-2018-11357, CVE-2018-11358, CVE-2018-11359, CVE-2018-11360, CVE-2018-11362

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.

23648 - Wireshark Multiple Vulnerabilities Prior To 2.6.1

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

Risk Level: Medium

CVE: CVE-2018-11354, CVE-2018-11355, CVE-2018-11356, CVE-2018-11357, CVE-2018-11358, CVE-2018-11359, CVE-2018-11360, CVE-2018-11361, CVE-2018-11362

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.

96055 - Red Hat Enterprise Linux RHSA-2018-1724 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2783, CVE-2018-2790, CVE-2018-2794, CVE-2018-2795, CVE-2018-2796, CVE-2018-2797, CVE-2018-2798, CVE-2018-2799, CVE-2018-2800

Description

The scan detected that the host is missing the following update:
RHSA-2018-1724

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00118.html

RHEL6D
x86_64
java-1.7.1-ibm-demo-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-jdbc-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-plugin-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-devel-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-src-1.7.1.4.25-1jpp.2.el6_9

i386
java-1.7.1-ibm-demo-1.7.1.4.25-1jpp.2.el6_9

java-1.7.1-ibm-jdbc-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-devel-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-plugin-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-src-1.7.1.4.25-1jpp.2.el6_9

RHEL6S
i386
java-1.7.1-ibm-demo-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-jdbc-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-devel-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-plugin-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-src-1.7.1.4.25-1jpp.2.el6_9

x86_64
java-1.7.1-ibm-demo-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-jdbc-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-devel-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-plugin-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-src-1.7.1.4.25-1jpp.2.el6_9

RHEL6WS
x86_64
java-1.7.1-ibm-demo-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-jdbc-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-devel-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-plugin-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-src-1.7.1.4.25-1jpp.2.el6_9

i386
java-1.7.1-ibm-demo-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-jdbc-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-devel-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-plugin-1.7.1.4.25-1jpp.2.el6_9
java-1.7.1-ibm-src-1.7.1.4.25-1jpp.2.el6_9

96056 - Red Hat Enterprise Linux RHSA-2018-1721 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2783, CVE-2018-2790, CVE-2018-2794, CVE-2018-2795, CVE-2018-2796, CVE-2018-2797, CVE-2018-2798, CVE-2018-2799, CVE-2018-2800

Description

The scan detected that the host is missing the following update:
RHSA-2018-1721

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00115.html

RHEL7D

x86_64
java-1.8.0-ibm-plugin-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-jdbc-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-devel-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-demo-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-src-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-1.8.0.5.15-1jpp.5.el7

RHEL7S
x86_64
java-1.8.0-ibm-plugin-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-jdbc-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-devel-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-demo-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-src-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-1.8.0.5.15-1jpp.5.el7

RHEL7WS
x86_64
java-1.8.0-ibm-plugin-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-jdbc-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-devel-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-demo-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-src-1.8.0.5.15-1jpp.5.el7
java-1.8.0-ibm-1.8.0.5.15-1jpp.5.el7

96061 - Red Hat Enterprise Linux RHSA-2018-1722 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2783, CVE-2018-2790, CVE-2018-2794, CVE-2018-2795, CVE-2018-2796, CVE-2018-2797, CVE-2018-2798, CVE-2018-2799, CVE-2018-2800

Description

The scan detected that the host is missing the following update:
RHSA-2018-1722

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00116.html

RHEL6D
x86_64
java-1.8.0-ibm-plugin-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-src-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-demo-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-jdbc-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-devel-1.8.0.5.15-1jpp.2.el6_9

i386
java-1.8.0-ibm-plugin-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-src-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-demo-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-jdbc-1.8.0.5.15-1jpp.2.el6_9

java-1.8.0-ibm-devel-1.8.0.5.15-1jpp.2.el6_9

RHEL6S
i386
java-1.8.0-ibm-plugin-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-src-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-demo-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-jdbc-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-devel-1.8.0.5.15-1jpp.2.el6_9

x86_64
java-1.8.0-ibm-plugin-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-src-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-demo-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-jdbc-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-devel-1.8.0.5.15-1jpp.2.el6_9

RHEL6WS
x86_64
java-1.8.0-ibm-plugin-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-src-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-demo-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-jdbc-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-devel-1.8.0.5.15-1jpp.2.el6_9

i386
java-1.8.0-ibm-plugin-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-src-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-demo-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-jdbc-1.8.0.5.15-1jpp.2.el6_9
java-1.8.0-ibm-devel-1.8.0.5.15-1jpp.2.el6_9

96069 - Red Hat Enterprise Linux RHSA-2018-1723 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2783, CVE-2018-2790, CVE-2018-2794, CVE-2018-2795, CVE-2018-2796, CVE-2018-2797, CVE-2018-2798, CVE-2018-2799, CVE-2018-2800

Description

The scan detected that the host is missing the following update:
RHSA-2018-1723

Observation

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

http://www.redhat.com/archives/rhsa-announce/2018-May/msg00117.html

RHEL7D
x86_64
java-1.7.1-ibm-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-jdbc-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-plugin-1.7.1.4.25-1jpp.3.el7

java-1.7.1-ibm-demo-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-devel-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-src-1.7.1.4.25-1jpp.3.el7

RHEL7S
x86_64
java-1.7.1-ibm-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-jdbc-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-plugin-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-demo-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-devel-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-src-1.7.1.4.25-1jpp.3.el7

RHEL7WS
x86_64
java-1.7.1-ibm-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-jdbc-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-plugin-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-demo-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-devel-1.7.1.4.25-1jpp.3.el7
java-1.7.1-ibm-src-1.7.1.4.25-1jpp.3.el7

132460 - Oracle VM OVMSA-2018-0223 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000410, CVE-2017-18203, CVE-2018-10323, CVE-2018-10675, CVE-2018-3639, CVE-2018-5333, CVE-2018-5750, CVE-2018-6927, CVE-2018-8781

Description

The scan detected that the host is missing the following update:
OVMSA-2018-0223

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2018-May/000858.html

OVM3.4
x86_64
kernel-uek-4.1.12-124.15.2.el6uek
kernel-uek-firmware-4.1.12-124.15.2.el6uek

146720 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1417-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-16818, CVE-2018-7262

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1417-1

Observation

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

For more information see:

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004086.html

SuSE SLED 12 SP3
x86_64
librados2-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
ceph-common-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-cephfs-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-rgw-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-cephfs-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
ceph-common-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-rados-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
ceph-debugsource-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-rgw-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
libradosstriper1-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
librados2-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
librgw2-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
librbd1-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-rados-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
libcephfs2-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-rbd-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
librgw2-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-rbd-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
libradosstriper1-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
libcephfs2-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
librbd1-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3

SuSE SLES 12 SP3
x86_64
librados2-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
ceph-common-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-cephfs-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-rgw-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-cephfs-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
ceph-common-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-rados-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
ceph-debugsource-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-rgw-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
libradosstriper1-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
librados2-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
librgw2-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
librbd1-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-rados-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
libcephfs2-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-rbd-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
librgw2-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
python-rbd-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
libradosstriper1-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
libcephfs2-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3
librbd1-debuginfo-12.2.5+git.1524775272.5e7ea8cf03-2.6.3

146730 - SuSE Linux 15.0, 42.3 openSUSE-SU-2018:1428-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11356, CVE-2018-11357, CVE-2018-11358, CVE-2018-11359, CVE-2018-11360, CVE-2018-11362

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1428-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00118.html

SuSE Linux 15.0
x86_64
libwireshark9-debuginfo-2.4.7-lp150.2.3.1
libwsutil8-debuginfo-2.4.7-lp150.2.3.1
libwiretap7-2.4.7-lp150.2.3.1
libwiretap7-debuginfo-2.4.7-lp150.2.3.1
wireshark-2.4.7-lp150.2.3.1
wireshark-ui-qt-2.4.7-lp150.2.3.1
libwscodecs1-2.4.7-lp150.2.3.1
libwsutil8-2.4.7-lp150.2.3.1
wireshark-debuginfo-2.4.7-lp150.2.3.1
wireshark-ui-qt-debuginfo-2.4.7-lp150.2.3.1
libwscodecs1-debuginfo-2.4.7-lp150.2.3.1
wireshark-devel-2.4.7-lp150.2.3.1
wireshark-debugsource-2.4.7-lp150.2.3.1
libwireshark9-2.4.7-lp150.2.3.1

SuSE Linux 42.3
x86_64
wireshark-ui-qt-2.2.15-41.1
wireshark-ui-gtk-debuginfo-2.2.15-41.1
wireshark-debugsource-2.2.15-41.1
wireshark-ui-gtk-2.2.15-41.1
wireshark-ui-qt-debuginfo-2.2.15-41.1
wireshark-debuginfo-2.2.15-41.1
wireshark-devel-2.2.15-41.1
wireshark-2.2.15-41.1

146732 - SuSE SLES 11 SP4 SUSE-SU-2018:1453-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9082, CVE-2017-7475, CVE-2017-9814

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1453-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004095.html

SuSE SLES 11 SP4
i586
cairo-doc-1.8.8-2.3.7.1
cairo-1.8.8-2.3.7.1

x86_64
cairo-doc-1.8.8-2.3.7.1
cairo-32bit-1.8.8-2.3.7.1
cairo-1.8.8-2.3.7.1

163631 - Oracle Enterprise Linux ELSA-2018-4114 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000410, CVE-2017-18203, CVE-2018-10323, CVE-2018-10675, CVE-2018-3639, CVE-2018-5333, CVE-2018-5750, CVE-2018-6927, CVE-2018-8781

Description

The scan detected that the host is missing the following update:
ELSA-2018-4114

Observation

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

http://oss.oracle.com/pipermail/el-errata/2018-May/007760.html
http://oss.oracle.com/pipermail/el-errata/2018-May/007761.html

OEL7
x86_64
kernel-uek-debug-devel-4.1.12-124.15.2.el7uek
kernel-uek-doc-4.1.12-124.15.2.el7uek
kernel-uek-debug-4.1.12-124.15.2.el7uek
kernel-uek-devel-4.1.12-124.15.2.el7uek
kernel-uek-firmware-4.1.12-124.15.2.el7uek
kernel-uek-4.1.12-124.15.2.el7uek

OEL6
x86_64
kernel-uek-debug-4.1.12-124.15.2.el6uek
kernel-uek-devel-4.1.12-124.15.2.el6uek
kernel-uek-debug-devel-4.1.12-124.15.2.el6uek
kernel-uek-4.1.12-124.15.2.el6uek
kernel-uek-firmware-4.1.12-124.15.2.el6uek
kernel-uek-doc-4.1.12-124.15.2.el6uek

170978 - Amazon Linux AMI ALAS-2018-1025 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-9234

Description

The scan detected that the host is missing the following update:
ALAS-2018-1025

Observation

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

https://alas.aws.amazon.com/ALAS-2018-1025.html

Amazon Linux AMI
x86_64
gnupg2-2.0.28-2.31.amzn1
gnupg2-debuginfo-2.0.28-2.31.amzn1
gnupg2-smime-2.0.28-2.31.amzn1

i686
gnupg2-2.0.28-2.31.amzn1
gnupg2-debuginfo-2.0.28-2.31.amzn1
gnupg2-smime-2.0.28-2.31.amzn1

178635 - Gentoo Linux GLSA-201805-12 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201805-12

Observation

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

https://security.gentoo.org/glsa/201805-12

Affected packages:
net-misc/ntp < 4.2.8_p11

178636 - Gentoo Linux GLSA-201805-11 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201805-11

Observation

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

https://security.gentoo.org/glsa/201805-11

Affected packages:
app-forensics/rkhunter < 1.4.6

178637 - Gentoo Linux GLSA-201805-10 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
GLSA-201805-10

Observation

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

https://security.gentoo.org/glsa/201805-10

Affected packages:
app-shells/zsh < 5.5

23637 - (K10329515) F5 BIG-IP PEM Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2018-5508

Description

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

Observation

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

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the Traffic Management Microkernel (TMM). Successful exploitation could allow remote attackers to cause a denial of service.

146710 - SuSE Linux 42.3 openSUSE-SU-2018:1440-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-9055

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1440-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00130.html

SuSE Linux 42.3
x86_64
jasper-debugsource-1.900.14-182.1
libjasper1-1.900.14-182.1
libjasper1-debuginfo-1.900.14-182.1
jasper-debuginfo-1.900.14-182.1
libjasper1-32bit-1.900.14-182.1
libjasper-devel-1.900.14-182.1
libjasper1-debuginfo-32bit-1.900.14-182.1
jasper-1.900.14-182.1

i586
jasper-debugsource-1.900.14-182.1
libjasper1-1.900.14-182.1
libjasper1-debuginfo-1.900.14-182.1
jasper-debuginfo-1.900.14-182.1
libjasper-devel-1.900.14-182.1
jasper-1.900.14-182.1

146716 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1424-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-9055

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1424-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004087.html

SuSE SLED 12 SP3
x86_64
jasper-debuginfo-1.900.14-195.8.1
jasper-debugsource-1.900.14-195.8.1
libjasper1-debuginfo-32bit-1.900.14-195.8.1
libjasper1-32bit-1.900.14-195.8.1
libjasper1-debuginfo-1.900.14-195.8.1
libjasper1-1.900.14-195.8.1

SuSE SLES 12 SP3
x86_64
jasper-debuginfo-1.900.14-195.8.1
jasper-debugsource-1.900.14-195.8.1
libjasper1-debuginfo-32bit-1.900.14-195.8.1
libjasper1-32bit-1.900.14-195.8.1
libjasper1-debuginfo-1.900.14-195.8.1
libjasper1-1.900.14-195.8.1

146719 - SuSE SLES 11 SP4 SUSE-SU-2018:1368-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2018-1000199, CVE-2018-10675, CVE-2018-3639

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1368-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004072.html

SuSE SLES 11 SP4
i586
kernel-trace-3.0.101-108.48.1
kernel-syms-3.0.101-108.48.1
kernel-default-3.0.101-108.48.1
kernel-pae-3.0.101-108.48.1
kernel-pae-devel-3.0.101-108.48.1
kernel-default-devel-3.0.101-108.48.1
kernel-ec2-3.0.101-108.48.1
kernel-xen-devel-3.0.101-108.48.1
kernel-source-3.0.101-108.48.1
kernel-xen-base-3.0.101-108.48.1
kernel-pae-base-3.0.101-108.48.1
kernel-trace-devel-3.0.101-108.48.1
kernel-ec2-devel-3.0.101-108.48.1
kernel-xen-3.0.101-108.48.1
kernel-default-base-3.0.101-108.48.1
kernel-ec2-base-3.0.101-108.48.1
kernel-trace-base-3.0.101-108.48.1

x86_64
kernel-trace-3.0.101-108.48.1
kernel-syms-3.0.101-108.48.1
kernel-default-3.0.101-108.48.1
kernel-default-devel-3.0.101-108.48.1
kernel-ec2-3.0.101-108.48.1
kernel-xen-devel-3.0.101-108.48.1
kernel-source-3.0.101-108.48.1
kernel-xen-base-3.0.101-108.48.1
kernel-trace-devel-3.0.101-108.48.1
kernel-ec2-devel-3.0.101-108.48.1
kernel-xen-3.0.101-108.48.1
kernel-default-base-3.0.101-108.48.1
kernel-ec2-base-3.0.101-108.48.1
kernel-trace-base-3.0.101-108.48.1

146723 - SuSE Linux 42.3 openSUSE-SU-2018:1395-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11104

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2018:1395-1

Observation

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

http://lists.opensuse.org/opensuse-updates/2018-05/msg00092.html

SuSE Linux 42.3
x86_64
knot-debuginfo-1.6.5-5.3.1

knot-debugsource-1.6.5-5.3.1
knot-1.6.5-5.3.1

i586
knot-debuginfo-1.6.5-5.3.1
knot-debugsource-1.6.5-5.3.1
knot-1.6.5-5.3.1

146739 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:1366-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000199, CVE-2018-10087, CVE-2018-10124, CVE-2018-1065, CVE-2018-1130, CVE-2018-3639, CVE-2018-5803, CVE-2018-7492, CVE-2018-8781

Description

The scan detected that the host is missing the following update:
SUSE-SU-2018:1366-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2018-May/004070.html

SuSE SLED 12 SP3
x86_64
kernel-default-extra-4.4.131-94.29.1
kernel-default-debugsource-4.4.131-94.29.1
kernel-default-extra-debuginfo-4.4.131-94.29.1
kernel-syms-4.4.131-94.29.1
kernel-default-devel-4.4.131-94.29.1
kernel-default-debuginfo-4.4.131-94.29.1
kernel-default-4.4.131-94.29.1

noarch
kernel-source-4.4.131-94.29.1
kernel-macros-4.4.131-94.29.1
kernel-devel-4.4.131-94.29.1

SuSE SLES 12 SP3
noarch
kernel-source-4.4.131-94.29.1
kernel-macros-4.4.131-94.29.1
kernel-devel-4.4.131-94.29.1

x86_64
kernel-default-debugsource-4.4.131-94.29.1
kernel-default-base-4.4.131-94.29.1
kernel-default-debuginfo-4.4.131-94.29.1
kernel-syms-4.4.131-94.29.1
kernel-default-devel-4.4.131-94.29.1
kernel-default-4.4.131-94.29.1
kernel-default-base-debuginfo-4.4.131-94.29.1

170979 - Amazon Linux AMI ALAS-2018-1028 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2755, CVE-2018-2761, CVE-2018-2771, CVE-2018-2773, CVE-2018-2781, CVE-2018-2813, CVE-2018-2817, CVE-2018-2818, CVE-2018-2819

Description

The scan detected that the host is missing the following update:
ALAS-2018-1028

Observation

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

https://alas.aws.amazon.com/ALAS-2018-1028.html

Amazon Linux AMI
x86_64
mysql55-embedded-5.5.60-1.21.amzn1
mysql55-embedded-devel-5.5.60-1.21.amzn1
mysql55-5.5.60-1.21.amzn1
mysql55-debuginfo-5.5.60-1.21.amzn1
mysql55-test-5.5.60-1.21.amzn1
mysql-config-5.5.60-1.21.amzn1
mysql55-bench-5.5.60-1.21.amzn1
mysql55-devel-5.5.60-1.21.amzn1
mysql55-libs-5.5.60-1.21.amzn1
mysql55-server-5.5.60-1.21.amzn1

i686
mysql55-embedded-5.5.60-1.21.amzn1
mysql55-embedded-devel-5.5.60-1.21.amzn1
mysql55-5.5.60-1.21.amzn1
mysql55-debuginfo-5.5.60-1.21.amzn1
mysql55-test-5.5.60-1.21.amzn1
mysql55-libs-5.5.60-1.21.amzn1
mysql-config-5.5.60-1.21.amzn1
mysql55-bench-5.5.60-1.21.amzn1
mysql55-devel-5.5.60-1.21.amzn1
mysql55-server-5.5.60-1.21.amzn1

88946 - Slackware Linux 14.2 SSA:2018-142-03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1122, CVE-2018-1123, CVE-2018-1124, CVE-2018-1125, CVE-2018-1126

Description

The scan detected that the host is missing the following update:
SSA:2018-142-03

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=2018&m=slackware-security.390479

Slackware 14.2

x86_64
procps-ng-3.3.15-x86_64-1

i586
procps-ng-3.3.15-i586-1

88947 - Slackware Linux 14.2 SSA:2018-142-02 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
SSA:2018-142-02

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=2018&m=slackware-security.362865

Slackware 14.2
x86_64
mozilla-thunderbird-52.8.0-x86_64-1

i586
mozilla-thunderbird-52.8.0-i586-1

131115 - Debian Linux 9.0 DSA-4210-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
DSA-4210-1

Observation

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

http://www.debian.org/security/2018/dsa-4210

Debian 9.0
all
libxen-4.8_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u7
libxen-dev_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u7
xen-hypervisor-4.8-arm64_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u7
xen-hypervisor-4.8-amd64_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u7
xen-system-arm64_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u7
xenstore-utils_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u7
xen-system-armhf_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u7
xen-system-amd64_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u7
xen-utils-4.8_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u7

xen-utils-common_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u7
libxenstore3.0_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u7
xen-hypervisor-4.8-armhf_4.8.3+xsa262+shim4.10.0+comet3-1+deb9u7

131116 - Debian Linux 8.0, 9.0 DSA-4211-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-18266

Description

The scan detected that the host is missing the following update:
DSA-4211-1

Observation

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

http://www.debian.org/security/2018/dsa-4211

Debian 8.0
all
xdg-utils_1.1.0~rc1+git20111210-7.4+deb8u1

Debian 9.0
all
xdg-utils_1.1.1-1+deb9u1

131117 - Debian Linux 8.0, 9.0 DSA-4208-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1122, CVE-2018-1123, CVE-2018-1124, CVE-2018-1125, CVE-2018-1126

Description

The scan detected that the host is missing the following update:
DSA-4208-1

Observation

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

http://www.debian.org/security/2018/dsa-4208

Debian 8.0
all
procps_2:3.3.9-9+deb8u1

Debian 9.0
all
procps_2:3.3.12-3+deb9u1

131118 - Debian Linux 9.0 DSA-4209-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5159, CVE-2018-5161, CVE-2018-5162, CVE-2018-5168, CVE-2018-5170, CVE-2018-5178, CVE-2018-5183, CVE-2018-5184, CVE-2018-5185

Description

The scan detected that the host is missing the following update:
DSA-4209-1

Observation

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

http://www.debian.org/security/2018/dsa-4209

Debian 9.0
all
thunderbird_1:52.8.0-1~deb9u1

131119 - Debian Linux 8.0, 9.0 DSA-4212-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-11235

Description

The scan detected that the host is missing the following update:
DSA-4212-1

Observation

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

http://www.debian.org/security/2018/dsa-4212

Debian 8.0
all
git_1:2.1.4-2.1+deb8u6

Debian 9.0
all
git_1:2.11.0-3+deb9u3

170980 - Amazon Linux AMI ALAS-2018-1024 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1111

Description

The scan detected that the host is missing the following update:
ALAS-2018-1024

Observation

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

For more information see:

https://alas.aws.amazon.com/ALAS-2018-1024.html

Amazon Linux AMI
x86_64
dhcp-devel-4.1.1-53.P1.28.amzn1
dhcp-common-4.1.1-53.P1.28.amzn1
dhcp-4.1.1-53.P1.28.amzn1
dhclient-4.1.1-53.P1.28.amzn1
dhcp-debuginfo-4.1.1-53.P1.28.amzn1

i686
dhcp-devel-4.1.1-53.P1.28.amzn1
dhcp-common-4.1.1-53.P1.28.amzn1
dhcp-4.1.1-53.P1.28.amzn1
dhclient-4.1.1-53.P1.28.amzn1
dhcp-debuginfo-4.1.1-53.P1.28.amzn1

186228 - Ubuntu Linux 14.04, 16.04, 17.10, 18.04 USN-3658-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1122, CVE-2018-1123, CVE-2018-1124, CVE-2018-1125, CVE-2018-1126

Description

The scan detected that the host is missing the following update:
USN-3658-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-May/004410.html

Ubuntu 16.04

procps_3.3.10-4ubuntu2.4
libprocps4_3.3.10-4ubuntu2.4

Ubuntu 14.04

libprocps3_3.3.9-1ubuntu2.3
procps_3.3.9-1ubuntu2.3

Ubuntu 18.04

libprocps6_3.3.12-3ubuntu1.1
procps_3.3.12-3ubuntu1.1

Ubuntu 17.10

procps_3.3.12-1ubuntu2.1
libprocps6_3.3.12-1ubuntu2.1

186231 - Ubuntu Linux 14.04, 16.04, 17.10, 18.04 USN-3660-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5150, CVE-2018-5154, CVE-2018-5155, CVE-2018-5159, CVE-2018-5161, CVE-2018-5162, CVE-2018-5168, CVE-2018-5170, CVE-2018-5178, CVE-2018-5183, CVE-2018-5184, CVE-2018-5185

Description

The scan detected that the host is missing the following update:
USN-3660-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2018-May/004413.html

Ubuntu 16.04

thunderbird_52.8.0+build1-0ubuntu0.16.04.1

Ubuntu 14.04

thunderbird_52.8.0+build1-0ubuntu0.14.04.1

Ubuntu 18.04

thunderbird_52.8.0+build1-0ubuntu0.18.04.1

Ubuntu 17.10

thunderbird_52.8.0+build1-0ubuntu0.17.10.1

193730 - Fedora Linux 27 FEDORA-2018-de5de06754 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1124, CVE-2018-1126

Description

The scan detected that the host is missing the following update:
FEDORA-2018-de5de06754

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/2018/5/?count=200&page=2

Fedora Core 27

procps-ng-3.3.10-16.fc27

193731 - Fedora Linux 28 FEDORA-2018-3731a89e20 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-5388

Description

The scan detected that the host is missing the following update:
FEDORA-2018-3731a89e20

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/2018/5/?count=200&page=1

Fedora Core 28

strongswan-5.6.2-6.fc28

193734 - Fedora Linux 27 FEDORA-2018-5c92e2a4ad 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-2018-5c92e2a4ad

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/2018/5/?count=200&page=2

Fedora Core 27

firefox-60.0.1-1.fc27

193735 - Fedora Linux 28 FEDORA-2018-2c965abb15 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-1059

Description

The scan detected that the host is missing the following update:
FEDORA-2018-2c965abb15

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/2018/5/?count=200&page=2

Fedora Core 28

dpdk-17.11.2-1.fc28

193736 - Fedora Linux 28 FEDORA-2018-636f73964f Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-3750

Description

The scan detected that the host is missing the following update:
FEDORA-2018-636f73964f

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/2018/5/?count=200&page=2

Fedora Core 28

nodejs-deep-extend-0.5.1-1.fc28

193737 - Fedora Linux 28 FEDORA-2018-77fe2e20ad Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17688, CVE-2017-17689

Description

The scan detected that the host is missing the following update:
FEDORA-2018-77fe2e20ad

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/2018/5/?count=200&page=2

Fedora Core 28

thunderbird-enigmail-2.0.4-1.fc28

193738 - Fedora Linux 26 FEDORA-2018-c8f559e8c2 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-18266

Description

The scan detected that the host is missing the following update:
FEDORA-2018-c8f559e8c2

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/2018/5/?count=200&page=2

Fedora Core 26

xdg-utils-1.1.3-1.fc26

193739 - Fedora Linux 26 FEDORA-2018-6020628437 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17688, CVE-2017-17689

Description

The scan detected that the host is missing the following update:
FEDORA-2018-6020628437

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/2018/5/?count=200&page=1

Fedora Core 26

thunderbird-enigmail-2.0.4-1.fc26

193741 - Fedora Linux 28 FEDORA-2018-17a97bb25b Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10536, CVE-2018-10537, CVE-2018-10538, CVE-2018-10539, CVE-2018-10540

Description

The scan detected that the host is missing the following update:
FEDORA-2018-17a97bb25b

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/2018/5/?count=200&page=2

Fedora Core 28

wavpack-5.1.0-8.fc28

193743 - Fedora Linux 28 FEDORA-2018-5521156807 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10471, CVE-2018-10472, CVE-2018-10981, CVE-2018-10982, CVE-2018-3639, CVE-2018-8897

Description

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

FEDORA-2018-5521156807

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/2018/5/?count=200&page=2

Fedora Core 28

xen-4.10.1-3.fc28

193744 - Fedora Linux 28 FEDORA-2018-916dfe0d86 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-11237

Description

The scan detected that the host is missing the following update:
FEDORA-2018-916dfe0d86

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/2018/5/?count=200&page=1

Fedora Core 28

glibc-2.27-15.fc28

193745 - Fedora Linux 27 FEDORA-2018-bff20f864b 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-2018-bff20f864b

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/2018/5/?count=200&page=2

Fedora Core 27

thunderbird-52.8.0-1.fc27

193746 - Fedora Linux 28 FEDORA-2018-537c8312fc Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10322, CVE-2018-10323, CVE-2018-10840, CVE-2018-1108, CVE-2018-1120, CVE-2018-3639

Description

The scan detected that the host is missing the following update:
FEDORA-2018-537c8312fc

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/2018/5/?count=200&page=1

Fedora Core 28

kernel-4.16.12-300.fc28

193748 - Fedora Linux 28 FEDORA-2018-8ce90c8b24 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10322, CVE-2018-10323, CVE-2018-1108, CVE-2018-1120

Description

The scan detected that the host is missing the following update:
FEDORA-2018-8ce90c8b24

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/2018/5/?count=200&page=2

Fedora Core 28

kernel-4.16.10-300.fc28

193750 - Fedora Linux 27 FEDORA-2018-fd850e033d Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10196

Description

The scan detected that the host is missing the following update:
FEDORA-2018-fd850e033d

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/2018/5/?count=200&page=1

Fedora Core 27

graphviz-2.40.1-11.fc27

193751 - Fedora Linux 28 FEDORA-2018-3f177356b0 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-2018-3f177356b0

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/2018/5/?count=200&page=2

Fedora Core 28

firefox-60.0.1-1.fc28

193752 - Fedora Linux 28 FEDORA-2018-25674bb48e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10196

Description

The scan detected that the host is missing the following update:
FEDORA-2018-25674bb48e

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/2018/5/?count=200&page=1

Fedora Core 28

graphviz-2.40.1-22.fc28

193755 - Fedora Linux 27 FEDORA-2018-25525a9346 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17688, CVE-2017-17689

Description

The scan detected that the host is missing the following update:
FEDORA-2018-25525a9346

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/2018/5/?count=200&page=1

Fedora Core 27

thunderbird-enigmail-2.0.4-1.fc27

193756 - Fedora Linux 28 FEDORA-2018-ca9df6aaf1 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-2018-ca9df6aaf1

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/2018/5/?count=200&page=2

Fedora Core 28

thunderbird-52.8.0-1.fc28

193757 - Fedora Linux 28 FEDORA-2018-db0d3e157e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-10322, CVE-2018-10323, CVE-2018-1108, CVE-2018-1120, CVE-2018-3639

Description

The scan detected that the host is missing the following update:
FEDORA-2018-db0d3e157e

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/2018/5/?count=200&page=2

Fedora Core 28

kernel-4.16.11-300.fc28

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.

23589 - (APSB18-09) Vulnerabilities In Adobe Acrobat And Reader

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

Risk Level: High

CVE: CVE-2018-4947, CVE-2018-4948, CVE-2018-4949, CVE-2018-4950, CVE-2018-4951, CVE-2018-4952, CVE-2018-4953, CVE-2018-4954, CVE-2018-4955, CVE-2018-4956, CVE-2018-4957, CVE-2018-4958, CVE-2018-4959, CVE-2018-4960, CVE-2018-4961, CVE-2018-4962, CVE-2018-4963, CVE-2018-4964, CVE-2018-4965, CVE-2018-4966, CVE-2018-4967, CVE-2018-4968, CVE-2018-4969, CVE-2018-4970, CVE-2018-4971, CVE-2018-4972, CVE-2018-4973, CVE-2018-4974, CVE-2018-4975, CVE-2018-4976, CVE-2018-4977, CVE-2018-4978, CVE-2018-4979, CVE-2018-4980, CVE-2018-4981, CVE-2018-4982, CVE-2018-4983, CVE-2018-4984, CVE-2018-4985, CVE-2018-4986, CVE-2018-4987, CVE-2018-4988, CVE-2018-4989, CVE-2018-4990, CVE-2018-4993, CVE-2018-4995, CVE-2018-4996

Update Details

CVE is updated

193681 - Fedora Linux 27 FEDORA-2018-490f30ffa0 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13089, CVE-2017-13090, CVE-2018-0494, CVE-2018-1055, CVE-2018-10583

Update Details

Risk is updated CVE is updated

23340 - (SB10229) McAfee Threat Intelligence Exchange Server Linux Kernel Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-1000364, CVE-2017-1000379

Update Details

Observation is updated

182669 - FreeBSD FreeBSD Ipsec Crash Or Denial Of Service (c0c5afef-38db-11e8-8b7f-a4badb2f469b)

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

Risk Level: High

CVE: CVE-2018-6918

Update Details

Risk is updated

130828 - Debian Linux 8.0, 9.0 DSA-3923-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2834, CVE-2017-2835, CVE-2017-2836, CVE-2017-2837, CVE-2017-2838, CVE-2017-2839

Update Details

Risk is updated

130882 - Debian Linux 8.0, 9.0 DSA-3976-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2923, CVE-2017-2924

Update Details

Risk is updated

131088 - Debian Linux 9.0 DSA-4181-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-9846

Update Details

Risk is updated

145490 - SuSE SLED 12 SP2, 12 SP3 SUSE-SU-2017:2234-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2834, CVE-2017-2835, CVE-2017-2836, CVE-2017-2837, CVE-2017-2838, CVE-2017-2839

Update Details

Risk is updated

145940 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2537-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2923, CVE-2017-2924

Update Details

Risk is updated

146505 - SuSE Linux 42.3 openSUSE-SU-2018:0734-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12122, CVE-2017-14440, CVE-2017-14441, CVE-2017-14442, CVE-2017-14448, CVE-2017-14449, CVE-2017-14450

Update Details

Risk is updated

182231 - FreeBSD cURL Uninitialized Random Vulnerability (c40ca16c-4d9f-4d70-8b6c-4d53aeb8ead4)

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

Risk Level: Medium

CVE: CVE-2016-9594

Update Details

Risk is updated

182478 - FreeBSD Multiple Exploitable Heap-based Buffer Overflow Vulnerabilities Exists In FreeXL 1.0.3 (555cd806-b031-11e7-a369-14dae9d

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

Risk Level: Medium

CVE: CVE-2017-2923, CVE-2017-2924

Update Details

Risk is updated

182673 - FreeBSD roundcube IMAP Command Injection Vulnerability (48894ca9-3e6f-11e8-92f0-f0def167eeea)

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

Risk Level: Medium

CVE: CVE-2018-9846

Update Details

Risk is updated

192468 - Fedora Linux 26 FEDORA-2017-4bc09c2364 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2834, CVE-2017-2835, CVE-2017-2836, CVE-2017-2837, CVE-2017-2838, CVE-2017-2839

Update Details

Risk is updated

192490 - Fedora Linux 25 FEDORA-2017-ed31e1f941 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2834, CVE-2017-2835, CVE-2017-2836, CVE-2017-2837, CVE-2017-2838, CVE-2017-2839

Update Details

Risk is updated

193594 - Fedora Linux 27 FEDORA-2018-57fbdb1cb5 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-9846

Update Details

Risk is updated

193596 - Fedora Linux 26 FEDORA-2018-f6dc921a19 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2018-9846

Update Details
Risk is updated

193634 - Fedora Linux 28 FEDORA-2018-c279b3696f Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-9846

Update Details
Risk is updated

182666 - FreeBSD FreeBSD Vt Console Memory Disclosure (a5cf3ecd-38db-11e8-8b7f-a4badb2f469b)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-6917

Update Details
Risk is updated

130736 - Debian Linux 8.0 DSA-3817-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-9601

Update Details
Risk is updated

178461 - Gentoo Linux GLSA-201706-24 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-2016-9601

Update Details
Risk is updated

191666 - Fedora Linux 25 FEDORA-2017-15f85f1cf1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-9601

Update Details
Risk is updated

191668 - Fedora Linux 24 FEDORA-2017-5136456ce3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9601

Update Details

Risk is updated

70116 - scada.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

DELETED CHECKS

22586 - (HPESBHF03769) HPE Integrated Lights-Out Remote Vulnerability

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

Risk Level: High

CVE: CVE-2017-12542

ADDITIONAL NOTES

- **22586** - is replaced by FID 23626.

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.