2019-FEB-13
FSL version 7.6.95

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

194753 - Fedora Linux 29 FEDORA-2019-1fb1547321 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-15686, CVE-2018-15687, CVE-2018-15688, CVE-2018-16864, CVE-2018-16865, CVE-2018-16866

Description

The scan detected that the host is missing the following update:
FEDORA-2019-1fb1547321

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

systemd-239-11.git4dc7dce.fc29

24761 - (APSB19-07) Multiple vulnerabilities In Adobe Acrobat and Reader

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

Risk Level: High

CVE: CVE-2018-19725, CVE-2019-7018, CVE-2019-7019, CVE-2019-7020, CVE-2019-7021, CVE-2019-7022, CVE-2019-7023, CVE-2019-7024, CVE-2019-7025, CVE-2019-7026, CVE-2019-7027, CVE-2019-7028, CVE-2019-7029, CVE-2019-7030, CVE-2019-7031, CVE-2019-7032, CVE-2019-7033, CVE-2019-7034, CVE-2019-7035, CVE-2019-7036, CVE-2019-7037, CVE-2019-7038, CVE-2019-7039, CVE-2019-7040, CVE-2019-7041, CVE-2019-7042, CVE-2019-7043, CVE-2019-7044, CVE-2019-7045, CVE-2019-7046, CVE-2019-7047, CVE-2019-7048, CVE-2019-7049, CVE-2019-7050, CVE-2019-7051, CVE-2019-7052, CVE-2019-7053, CVE-2019-7054, CVE-2019-7055, CVE-2019-7056, CVE-2019-7057, CVE-2019-7058, CVE-2019-7059, CVE-2019-7060, CVE-2019-7062, CVE-2019-7063, CVE-2019-7064, CVE-2019-7065, CVE-2019-7066, CVE-2019-7067, CVE-2019-7068, CVE-2019-7069, CVE-2019-7070, CVE-2019-7071, CVE-2019-7072, CVE-2019-7073, CVE-2019-7074, CVE-2019-7075, CVE-2019-7076, CVE-2019-7077, CVE-2019-7078, CVE-2019-7079, CVE-2019-7080, CVE-2019-7081, CVE-2019-7082, CVE-2019-7084, CVE-2019-7085, CVE-2019-7086, CVE-2019-7087, CVE-2019-7089

Description

Multiple vulnerabilities are present in some versions of Adobe Reader and Acrobat.

Observation

Adobe Reader and Acrobat are popular applications used to handle PDF files.

Multiple vulnerabilities are present in some versions of Adobe Reader and Acrobat. The flaws lie in undetermined components. Successful exploitation could allow an attacker to obtain sensitive information, execute arbitrary code or obtain elevated privileges.

The update provided by Adobe bulletin APSB19-07 resolves these issues.

196249 - Red Hat Enterprise Linux RHSA-2019-0309 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5754, CVE-2019-5755, CVE-2019-5756, CVE-2019-5757, CVE-2019-5758, CVE-2019-5759, CVE-2019-5760, CVE-2019-5761, CVE-2019-5762, CVE-2019-5763, CVE-2019-5764, CVE-2019-5765, CVE-2019-5766, CVE-2019-5767, CVE-2019-5768, CVE-2019-5769, CVE-2019-5770, CVE-2019-5771, CVE-2019-5772, CVE-2019-5773, CVE-2019-5774, CVE-2019-5775, CVE-2019-5776, CVE-2019-5777, CVE-2019-5778, CVE-2019-5779, CVE-2019-5780, CVE-2019-5781, CVE-2019-5782

Description

The scan detected that the host is missing the following update:
RHSA-2019-0309

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-February/msg00008.html

RHEL6D
x86_64
chromium-browser-72.0.3626.81-1.el6_10
chromium-browser-debuginfo-72.0.3626.81-1.el6_10

i386
chromium-browser-72.0.3626.81-1.el6_10
chromium-browser-debuginfo-72.0.3626.81-1.el6_10

RHEL6S
x86_64
chromium-browser-72.0.3626.81-1.el6_10
chromium-browser-debuginfo-72.0.3626.81-1.el6_10

i386
chromium-browser-72.0.3626.81-1.el6_10
chromium-browser-debuginfo-72.0.3626.81-1.el6_10

RHEL6WS
x86_64
chromium-browser-72.0.3626.81-1.el6_10
chromium-browser-debuginfo-72.0.3626.81-1.el6_10

i386
chromium-browser-72.0.3626.81-1.el6_10
chromium-browser-debuginfo-72.0.3626.81-1.el6_10

24672 - (MSPT-Feb2019) Microsoft .NET Framework Remote Code Execution Vulnerability (CVE-2019-0613)

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

Risk Level: High

CVE: CVE-2019-0613

Description

A vulnerability in some versions of Microsoft .NET could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft .NET could lead to remote code execution.

The flaw is due to improper handing of the source markup of a file. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24689 - (MSPT-Feb2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution Vulnerability (CVE-2019-0640)

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

Risk Level: High

CVE: CVE-2019-0640

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies due the improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

24690 - (MSPT-Feb2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution Vulnerability (CVE-2019-0605)

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

Risk Level: High

CVE: CVE-2019-0605

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the scripting engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

24691 - (MSPT-Feb2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution Vulnerability (CVE-2019-0593)

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

Risk Level: High

CVE: CVE-2019-0593

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the scripting engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24692 - (MSPT-Feb2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution Vulnerability (CVE-2019-0591)

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

Risk Level: High

CVE: CVE-2019-0591

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the scripting engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24693 - (MSPT-Feb2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution Vulnerability (CVE-2019-0590)

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

Risk Level: High

CVE: CVE-2019-0590

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the scripting engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24694 - (MSPT-Feb2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0644)

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

Risk Level: High

CVE: CVE-2019-0644

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the improperly handles objects in the memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24697 - (MSPT-Feb2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0642)

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

Risk Level: High

CVE: CVE-2019-0642

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies due the improperly handles objects in the memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24698 - (MSPT-Feb2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution Vulnerability (CVE-2019-0651)

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

Risk Level: High

CVE: CVE-2019-0651

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the improperly handles objects in the memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24699 - (MSPT-Feb2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution Vulnerability (CVE-2019-0652)

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

Risk Level: High

CVE: CVE-2019-0652

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the improperly handles objects in the memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24700 - (MSPT-Feb2019) Microsoft Jet Database Engine Remote Code Execution Vulnerability (CVE-2019-0597)

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

Risk Level: High

CVE: CVE-2019-0597

Description

A vulnerability in some versions of Microsoft Jet Database Engine could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Jet Database Engine could lead to remote code execution.

The flaw lies in the improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24701 - (MSPT-Feb2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution Vulnerability (CVE-2019-0655)

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

Risk Level: High

CVE: CVE-2019-0655

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the improperly handles objects in the memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24702 - (MSPT-Feb2019) Microsoft Edge Improperly Handles Objects in Memory Remote Code Execution Vunerability (CVE-2019-0650)

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

Risk Level: High

CVE: CVE-2019-0650

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the improperly handles objects in the memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24703 - (MSPT-Feb2019) Microsoft Edge Scripting Engine Remote Code Execution Vulnerability (CVE-2019-0607)

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

Risk Level: High

CVE: CVE-2019-0607

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the scripting engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24704 - (MSPT-Feb2019) Microsoft Jet Database Engine Remote Code Execution Vulnerability (CVE-2019-0598)

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

Risk Level: High

CVE: CVE-2019-0598

Description

A vulnerability in some versions of Microsoft Jet Database Engine could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Jet Database Engine could lead to remote code execution.

The flaw lies in the improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24705 - (MSPT-Feb2019) Microsoft Jet Database Engine Remote Code Execution Vulnerability (CVE-2019-0599)

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

Risk Level: High

CVE: CVE-2019-0599

Description

A vulnerability in some versions of Microsoft Jet Database Engine could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Jet Database Engine could lead to remote code execution.

The flaw lies in the improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24706 - (MSPT-Feb2019) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2019-0625)

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

Risk Level: High

CVE: CVE-2019-0625

Description

A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

The flaw lies in the jet database engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24707 - (MSPT-Feb2019) Microsoft Jet Database Engine Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0595)

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

Risk Level: High

CVE: CVE-2019-0595

Description

A vulnerability in some versions of Microsoft Jet Database Engine could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Jet Database Engine could lead to remote code execution.

The flaw lies in the Improperly Handles Objects in Memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24708 - (MSPT-Feb2019) Microsoft Jet Database Engine Remote Code Execution Vulnerability (CVE-2019-0596)

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

Risk Level: High

CVE: CVE-2019-0596

Description

A vulnerability in some versions of Microsoft Jet Database Engine could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Jet Database Engine could lead to remote code execution.

The flaw lies in the improperly handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24711 - (MSPT-Feb2019) Microsoft Office Access Connectivity Engine Remote Code Execution (CVE-2019-0671)

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

Risk Level: High

CVE: CVE-2019-0671

Description

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

The flaw lies in the access connectivity engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24712 - (MSPT-Feb2019) Microsoft Office Access Connectivity Engine Remote Code Execution (CVE-2019-0672)

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

Risk Level: High

CVE: CVE-2019-0672

Description

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

The flaw lies in the access connectivity engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24713 - (MSPT-Feb2019) Microsoft Office Access Connectivity Engine Remote Code Execution (CVE-2019-0673)

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

Risk Level: High

CVE: CVE-2019-0673

Description

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

The flaw lies in the access connectivity engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24714 - (MSPT-Feb2019) Microsoft Office Access Connectivity Engine Remote Code Execution (CVE-2019-0674)

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

Risk Level: High

CVE: CVE-2019-0674

Description

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

The flaw lies in the access connectivity engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24718 - (MSPT-Feb2019) Microsoft Windows Graphics Device Interface Remote Code Execution (CVE-2019-0662)

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

Risk Level: High

CVE: CVE-2019-0662

Description

A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

The flaw lies in the graphics device interface component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24720 - (MSPT-Feb2019) Microsoft Windows GDI Remote Code Execution (CVE-2019-0618)

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

Risk Level: High

CVE: CVE-2019-0618

Description

A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Windows could lead to remote code execution.

The flaw lies in the gdi component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24724 - (MSPT-Feb2019) Microsoft SMBv2 Remote Code Execution Vulnerability (CVE-2019-0630)

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

Risk Level: High

CVE: CVE-2019-0630

Description

A vulnerability in some versions of Microsoft could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft could lead to remote code execution.

The flaw lies in the smbv2 server component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.

24725 - (MSPT-Feb2019) Microsoft SMBv2 Remote Code Execution Vulnerability (CVE-2019-0633)

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

Risk Level: High

CVE: CVE-2019-0633

Description

A vulnerability in some versions of Microsoft SMBv2 could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft SMBv2 could lead to remote code execution.

The flaw is due to improperly handles requests. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.

24727 - (MSPT-Feb2019) Microsoft Internet Explorer Remote Code Execution Vulnerability (CVE-2019-0606)

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

Risk Level: High

CVE: CVE-2019-0606

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

The flaw lies in the Microsoft Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

24732 - (MSPT-Feb2019) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2019-0610)

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

Risk Level: High

CVE: CVE-2019-0610

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the scripting engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

24733 - (MSPT-Feb2019) Microsoft Edge Memory Corruption Remote Code Execution Vulnerability (CVE-2019-0634)

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

Risk Level: High

CVE: CVE-2019-0634

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw is due to Improperly Accessing Objects in the Memory component. Successful exploitation by an attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24739 - (MSPT-Feb2019) Microsoft SharePoint Fails Check Application Package Remote Code Execution (CVE-2019-0604)

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

Risk Level: High

CVE: CVE-2019-0604

Description

A vulnerability in some versions of Microsoft SharePoint could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft SharePoint could lead to remote code execution.

The flaw lies when the software fails to check the source markup of an application package. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

24740 - (MSPT-Feb2019) Microsoft SharePoint Fails Check Application Package Remote Code Execution (CVE-2019-0594)

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

Risk Level: High

CVE: CVE-2019-0594

Description

A vulnerability in some versions of Microsoft SharePoint could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Share Point could lead to remote code execution.

The flaw lies when the software fails to check the source markup of an application package. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

24758 - (MSPT-Feb2019) Microsoft Team Foundation Server Cross-site Scripting Vulnerability (CVE-2019-0742)

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

Risk Level: High

CVE: CVE-2019-0742

Description

A vulnerability in some versions of Microsoft Team Foundation Server could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Team Foundation Server could lead to remote code execution.

The flaw is due to improper handling of user provided input. Successful exploitation by an authenticated attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24759 - (MSPT-Feb2019) Microsoft Team Foundation Server Cross-site Scripting Vulnerability (CVE-2019-0743)

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

Risk Level: High

CVE: CVE-2019-0743

Description

A vulnerability in some versions of Microsoft Team Foundation Server could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Team Foundation Server could lead to remote code execution.

The flaw is due to improper handling of user provided input. Successful exploitation by an authenticated attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24762 - (APSB19-06) Vulnerability In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2019-7090

Description

An information disclosure vulnerability is present in some versions of Adobe Flash Player.

Observation

Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files.

An information disclosure vulnerability is present in some versions of Adobe Flash Player. Successful exploitation could allow an attacker to obtain sensitive information.

The update provided by Adobe bulletin APSB19-06 resolves the issue. The target system is missing this update.

89002 - Slackware Linux 14.0, 14.1, 14.2 SSA:2019-037-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16890, CVE-2019-3822, CVE-2019-3823

Description

The scan detected that the host is missing the following update:
SSA:2019-037-01

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=2019&m=slackware-security.433275

Slackware 14.0
x86_64
curl-7.64.0-x86_64-1

Slackware 14.2
x86_64
curl-7.64.0-x86_64-1

i586
curl-7.64.0-i586-1

Slackware 14.1
x86_64
curl-7.64.0-x86_64-1

131294 - Debian Linux 9.0 DSA-4386-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16890, CVE-2019-3822, CVE-2019-3823

Description

The scan detected that the host is missing the following update:
DSA-4386-1

Observation

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

http://www.debian.org/security/2019/dsa-4386

Debian 9.0
all
curl_7.52.1-5+deb9u9

147604 - SuSE SLES 12 SP3, 12 SP4 SUSE-SU-2019:0313-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20748, CVE-2018-20749, CVE-2018-20750

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0313-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005100.html

SuSE SLES 12 SP3
x86_64
libvncclient0-debuginfo-0.9.9-17.11.1
LibVNCServer-debugsource-0.9.9-17.11.1
libvncserver0-debuginfo-0.9.9-17.11.1
libvncclient0-0.9.9-17.11.1
libvncserver0-0.9.9-17.11.1

SuSE SLES 12 SP4

x86_64
libvncclient0-debuginfo-0.9.9-17.11.1
LibVNCServer-debugsource-0.9.9-17.11.1
libvncserver0-debuginfo-0.9.9-17.11.1
libvncclient0-0.9.9-17.11.1
libvncserver0-0.9.9-17.11.1

147605 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0336-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0336-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005108.html

SuSE SLED 12 SP3
x86_64
mozilla-nss-certs-32bit-3.41.1-58.25.1
mozilla-nss-3.41.1-58.25.1
libsoftokn3-debuginfo-3.41.1-58.25.1
MozillaFirefox-60.5.0esr-109.58.3
mozilla-nss-tools-3.41.1-58.25.1
MozillaFirefox-debuginfo-60.5.0esr-109.58.3
MozillaFirefox-debugsource-60.5.0esr-109.58.3
libfreebl3-debuginfo-32bit-3.41.1-58.25.1
mozilla-nss-tools-debuginfo-3.41.1-58.25.1
libfreebl3-32bit-3.41.1-58.25.1
libsoftokn3-3.41.1-58.25.1
mozilla-nss-certs-debuginfo-32bit-3.41.1-58.25.1
libfreebl3-3.41.1-58.25.1
mozilla-nss-sysinit-3.41.1-58.25.1
libfreebl3-debuginfo-3.41.1-58.25.1
mozilla-nss-debugsource-3.41.1-58.25.1
mozilla-nss-32bit-3.41.1-58.25.1
mozilla-nss-sysinit-debuginfo-32bit-3.41.1-58.25.1
mozilla-nss-debuginfo-3.41.1-58.25.1
libsoftokn3-32bit-3.41.1-58.25.1
MozillaFirefox-translations-common-60.5.0esr-109.58.3
mozilla-nss-sysinit-32bit-3.41.1-58.25.1
mozilla-nss-debuginfo-32bit-3.41.1-58.25.1
mozilla-nss-certs-debuginfo-3.41.1-58.25.1
MozillaFirefox-branding-SLE-60-32.5.1
libsoftokn3-debuginfo-32bit-3.41.1-58.25.1
mozilla-nss-sysinit-debuginfo-3.41.1-58.25.1
mozilla-nss-certs-3.41.1-58.25.1

SuSE SLED 12 SP4
x86_64
mozilla-nss-certs-32bit-3.41.1-58.25.1
mozilla-nss-3.41.1-58.25.1

libsoftokn3-debuginfo-3.41.1-58.25.1
MozillaFirefox-60.5.0esr-109.58.3
mozilla-nss-tools-3.41.1-58.25.1
MozillaFirefox-debuginfo-60.5.0esr-109.58.3
MozillaFirefox-debugsource-60.5.0esr-109.58.3
libfreebl3-debuginfo-32bit-3.41.1-58.25.1
mozilla-nss-tools-debuginfo-3.41.1-58.25.1
libfreebl3-32bit-3.41.1-58.25.1
libsoftokn3-3.41.1-58.25.1
mozilla-nss-certs-debuginfo-32bit-3.41.1-58.25.1
libfreebl3-3.41.1-58.25.1
mozilla-nss-sysinit-3.41.1-58.25.1
libfreebl3-debuginfo-3.41.1-58.25.1
mozilla-nss-debugsource-3.41.1-58.25.1
mozilla-nss-32bit-3.41.1-58.25.1
mozilla-nss-sysinit-debuginfo-32bit-3.41.1-58.25.1
mozilla-nss-debuginfo-3.41.1-58.25.1
libsoftokn3-32bit-3.41.1-58.25.1
MozillaFirefox-translations-common-60.5.0esr-109.58.3
mozilla-nss-sysinit-32bit-3.41.1-58.25.1
mozilla-nss-debuginfo-32bit-3.41.1-58.25.1
mozilla-nss-certs-debuginfo-3.41.1-58.25.1
MozillaFirefox-branding-SLE-60-32.5.1
libsoftokn3-debuginfo-32bit-3.41.1-58.25.1
mozilla-nss-sysinit-debuginfo-3.41.1-58.25.1
mozilla-nss-certs-3.41.1-58.25.1

SuSE SLES 12 SP4
x86_64
mozilla-nss-certs-32bit-3.41.1-58.25.1
mozilla-nss-3.41.1-58.25.1
libsoftokn3-debuginfo-3.41.1-58.25.1
MozillaFirefox-60.5.0esr-109.58.3
mozilla-nss-tools-3.41.1-58.25.1
libfreebl3-hmac-32bit-3.41.1-58.25.1
MozillaFirefox-debuginfo-60.5.0esr-109.58.3
MozillaFirefox-debugsource-60.5.0esr-109.58.3
libfreebl3-debuginfo-32bit-3.41.1-58.25.1
mozilla-nss-tools-debuginfo-3.41.1-58.25.1
libsoftokn3-3.41.1-58.25.1
mozilla-nss-certs-debuginfo-32bit-3.41.1-58.25.1
libfreebl3-3.41.1-58.25.1
mozilla-nss-sysinit-3.41.1-58.25.1
libfreebl3-debuginfo-3.41.1-58.25.1
mozilla-nss-sysinit-32bit-3.41.1-58.25.1
mozilla-nss-debugsource-3.41.1-58.25.1
mozilla-nss-32bit-3.41.1-58.25.1
libsoftokn3-hmac-32bit-3.41.1-58.25.1
mozilla-nss-debuginfo-3.41.1-58.25.1
libsoftokn3-32bit-3.41.1-58.25.1
MozillaFirefox-translations-common-60.5.0esr-109.58.3
mozilla-nss-debuginfo-32bit-3.41.1-58.25.1
mozilla-nss-certs-3.41.1-58.25.1
libsoftokn3-hmac-3.41.1-58.25.1
mozilla-nss-certs-debuginfo-3.41.1-58.25.1
mozilla-nss-sysinit-debuginfo-32bit-3.41.1-58.25.1
MozillaFirefox-branding-SLE-60-32.5.1
libsoftokn3-debuginfo-32bit-3.41.1-58.25.1
libfreebl3-hmac-3.41.1-58.25.1
mozilla-nss-sysinit-debuginfo-3.41.1-58.25.1

libfreebl3-32bit-3.41.1-58.25.1

SuSE SLES 12 SP3
x86_64
mozilla-nss-certs-32bit-3.41.1-58.25.1
mozilla-nss-3.41.1-58.25.1
libsoftokn3-debuginfo-3.41.1-58.25.1
MozillaFirefox-60.5.0esr-109.58.3
mozilla-nss-tools-3.41.1-58.25.1
libfreebl3-hmac-32bit-3.41.1-58.25.1
MozillaFirefox-debuginfo-60.5.0esr-109.58.3
MozillaFirefox-debugsource-60.5.0esr-109.58.3
libfreebl3-debuginfo-32bit-3.41.1-58.25.1
mozilla-nss-tools-debuginfo-3.41.1-58.25.1
libsoftokn3-3.41.1-58.25.1
mozilla-nss-certs-debuginfo-32bit-3.41.1-58.25.1
libfreebl3-3.41.1-58.25.1
mozilla-nss-sysinit-3.41.1-58.25.1
libfreebl3-debuginfo-3.41.1-58.25.1
mozilla-nss-sysinit-32bit-3.41.1-58.25.1
mozilla-nss-debugsource-3.41.1-58.25.1
mozilla-nss-32bit-3.41.1-58.25.1
libsoftokn3-hmac-32bit-3.41.1-58.25.1
mozilla-nss-debuginfo-3.41.1-58.25.1
libsoftokn3-32bit-3.41.1-58.25.1
MozillaFirefox-translations-common-60.5.0esr-109.58.3
mozilla-nss-debuginfo-32bit-3.41.1-58.25.1
mozilla-nss-certs-3.41.1-58.25.1
libsoftokn3-hmac-3.41.1-58.25.1
mozilla-nss-certs-debuginfo-3.41.1-58.25.1
mozilla-nss-sysinit-debuginfo-32bit-3.41.1-58.25.1
MozillaFirefox-branding-SLE-60-32.5.1
libsoftokn3-debuginfo-32bit-3.41.1-58.25.1
libfreebl3-hmac-3.41.1-58.25.1
mozilla-nss-sysinit-debuginfo-3.41.1-58.25.1
libfreebl3-32bit-3.41.1-58.25.1

147608 - SuSE SLES 11 SP4 SUSE-SU-2019:13952-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20748, CVE-2018-20749, CVE-2018-20750

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13952-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005107.html

SuSE SLES 11 SP4
i586
LibVNCServer-0.9.1-160.9.1

x86_64

LibVNCServer-0.9.1-160.9.1

147610 - SuSE SLES 11 SP4 SUSE-SU-2019:13947-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1000845

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13947-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005098.html

SuSE SLES 11 SP4
i586
avahi-0.6.23-35.6.2
libdns_sd-0.6.23-35.6.2
avahi-utils-0.6.23-35.6.2
libavahi-core5-0.6.23-35.6.2
libavahi-common3-0.6.23-35.6.2
libavahi-glib1-0.6.23-35.6.1
libavahi-client3-0.6.23-35.6.2
avahi-lang-0.6.23-35.6.2

x86_64
libdns_sd-32bit-0.6.23-35.6.2
avahi-0.6.23-35.6.2
libdns_sd-0.6.23-35.6.2
libavahi-glib1-32bit-0.6.23-35.6.1
avahi-utils-0.6.23-35.6.2
libavahi-core5-0.6.23-35.6.2
libavahi-common3-0.6.23-35.6.2
libavahi-glib1-0.6.23-35.6.1
libavahi-client3-0.6.23-35.6.2
libavahi-common3-32bit-0.6.23-35.6.2
libavahi-client3-32bit-0.6.23-35.6.2
avahi-lang-0.6.23-35.6.2

147611 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2019:0249-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16890, CVE-2019-3822, CVE-2019-3823

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0249-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005088.html

SuSE SLED 12 SP3
x86_64
curl-debuginfo-7.37.0-37.34.1
libcurl4-7.37.0-37.34.1
libcurl4-debuginfo-7.37.0-37.34.1
curl-debugsource-7.37.0-37.34.1
curl-7.37.0-37.34.1
libcurl4-32bit-7.37.0-37.34.1
libcurl4-debuginfo-32bit-7.37.0-37.34.1

SuSE SLES 12 SP3
x86_64
curl-debuginfo-7.37.0-37.34.1
libcurl4-7.37.0-37.34.1
libcurl4-debuginfo-7.37.0-37.34.1
curl-debugsource-7.37.0-37.34.1
curl-7.37.0-37.34.1
libcurl4-32bit-7.37.0-37.34.1
libcurl4-debuginfo-32bit-7.37.0-37.34.1

147613 - SuSE SLED 15 SUSE-SU-2019:0283-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20748, CVE-2018-20749, CVE-2018-20750

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0283-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005096.html

SuSE SLED 15
x86_64
LibVNCServer-debugsource-0.9.10-4.6.1
libvncclient0-debuginfo-0.9.10-4.6.1
libvncclient0-0.9.10-4.6.1

147614 - SuSE SLES 12 SP3 SUSE-SU-2019:0320-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-16939, CVE-2018-1120, CVE-2018-16862, CVE-2018-16884, CVE-2018-19407, CVE-2018-19824, CVE-2018-19985, CVE-2018-20169, CVE-2018-9568

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0320-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005101.html

SuSE SLES 12 SP3
x86_64
dlm-kmp-rt-4.4.170-3.32.2
cluster-md-kmp-rt-4.4.170-3.32.2
kernel-rt-base-debuginfo-4.4.170-3.32.2
dlm-kmp-rt-debuginfo-4.4.170-3.32.2
kernel-rt-debugsource-4.4.170-3.32.2
kernel-rt-debuginfo-4.4.170-3.32.2
kernel-rt-4.4.170-3.32.2
kernel-rt_debug-devel-4.4.170-3.32.2
kernel-syms-rt-4.4.170-3.32.1
ocfs2-kmp-rt-4.4.170-3.32.2
kernel-rt_debug-debuginfo-4.4.170-3.32.2
kernel-rt_debug-debugsource-4.4.170-3.32.2
gfs2-kmp-rt-debuginfo-4.4.170-3.32.2
gfs2-kmp-rt-4.4.170-3.32.2
kernel-rt-devel-4.4.170-3.32.2
ocfs2-kmp-rt-debuginfo-4.4.170-3.32.2
kernel-rt_debug-devel-debuginfo-4.4.170-3.32.2
kernel-rt-base-4.4.170-3.32.2
cluster-md-kmp-rt-debuginfo-4.4.170-3.32.2

noarch
kernel-source-rt-4.4.170-3.32.1
kernel-devel-rt-4.4.170-3.32.1

147615 - SuSE SLES 11 SP4 SUSE-SU-2019:13951-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6446

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13951-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005104.html

SuSE SLES 11 SP4
i586
python-numpy-1.8.0-6.4.1

x86_64
python-numpy-1.8.0-6.4.1

147619 - SuSE Linux 42.3 openSUSE-SU-2019:0140-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1120, CVE-2018-16862, CVE-2018-16884, CVE-2018-19407, CVE-2018-19824, CVE-2018-19985, CVE-2018-20169, CVE-2018-9568, CVE-2019-3459, CVE-2019-3460

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0140-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00031.html

SuSE Linux 42.3
x86_64
kernel-default-base-4.4.172-86.1
kernel-debug-4.4.172-86.1
kernel-vanilla-base-4.4.172-86.1
kernel-vanilla-debuginfo-4.4.172-86.1
kernel-default-4.4.172-86.1
kernel-default-base-debuginfo-4.4.172-86.1
kernel-debug-devel-debuginfo-4.4.172-86.1
kernel-vanilla-debugsource-4.4.172-86.1
kernel-vanilla-devel-4.4.172-86.1
kernel-syms-4.4.172-86.1
kernel-default-debugsource-4.4.172-86.1
kernel-vanilla-4.4.172-86.1
kernel-debug-debuginfo-4.4.172-86.1
kernel-debug-devel-4.4.172-86.1
kernel-obs-qa-4.4.172-86.1
kernel-vanilla-base-debuginfo-4.4.172-86.1
kernel-default-debuginfo-4.4.172-86.1
kernel-obs-build-debugsource-4.4.172-86.1
kernel-debug-debugsource-4.4.172-86.1
kernel-debug-base-4.4.172-86.1
kernel-debug-base-debuginfo-4.4.172-86.1
kernel-obs-build-4.4.172-86.1
kernel-default-devel-4.4.172-86.1

noarch
kernel-docs-4.4.172-86.1
kernel-docs-pdf-4.4.172-86.1
kernel-docs-html-4.4.172-86.1
kernel-devel-4.4.172-86.1
kernel-source-4.4.172-86.1
kernel-macros-4.4.172-86.1
kernel-source-vanilla-4.4.172-86.1

147620 - SuSE SLED 15 SUSE-SU-2019:0338-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5824, CVE-2018-12405, CVE-2018-17466, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18498, CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0338-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005110.html

SuSE SLED 15
x86_64
MozillaThunderbird-debugsource-60.5.0-3.20.2
MozillaThunderbird-60.5.0-3.20.2
MozillaThunderbird-debuginfo-60.5.0-3.20.2
MozillaThunderbird-translations-other-60.5.0-3.20.2
MozillaThunderbird-translations-common-60.5.0-3.20.2

147621 - SuSE Linux 15.0 openSUSE-SU-2019:0143-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6690

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0143-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00034.html

SuSE Linux 15.0
noarch
python3-python-gnupg-0.4.4-lp150.2.6.1
python2-python-gnupg-0.4.4-lp150.2.6.1

160515 - CentOS 6 CESA-2019-0269 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5824, CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Description

The scan detected that the host is missing the following update:
CESA-2019-0269

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-February/023190.html

CentOS 6
x86_64
thunderbird-60.5.0-1.el6.centos

i686
thunderbird-60.5.0-1.el6.centos

160516 - CentOS 7 CESA-2019-0270 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-5824, CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Description

The scan detected that the host is missing the following update:
CESA-2019-0270

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-February/023193.html

CentOS 7
x86_64
thunderbird-60.5.0-1.el7.centos

163803 - Oracle Enterprise Linux ELSA-2019-4532 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18204, CVE-2018-1094, CVE-2018-14609, CVE-2018-17972

Description

The scan detected that the host is missing the following update:
ELSA-2019-4532

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-February/008474.html
http://oss.oracle.com/pipermail/el-errata/2019-February/008475.html

OEL7
x86_64
kernel-uek-3.8.13-118.30.1.el7uek
kernel-uek-debug-devel-3.8.13-118.30.1.el7uek
kernel-uek-debug-3.8.13-118.30.1.el7uek
kernel-uek-devel-3.8.13-118.30.1.el7uek
dtrace-modules-3.8.13-118.30.1.el7uek-0.4.5-3.el7
kernel-uek-firmware-3.8.13-118.30.1.el7uek
kernel-uek-doc-3.8.13-118.30.1.el7uek

OEL6
x86_64

dtrace-modules-3.8.13-118.30.1.el6uek-0.4.5-3.el6
kernel-uek-firmware-3.8.13-118.30.1.el6uek
kernel-uek-debug-3.8.13-118.30.1.el6uek
kernel-uek-3.8.13-118.30.1.el6uek
kernel-uek-debug-devel-3.8.13-118.30.1.el6uek
kernel-uek-devel-3.8.13-118.30.1.el6uek
kernel-uek-doc-3.8.13-118.30.1.el6uek

163805 - Oracle Enterprise Linux ELSA-2019-4533 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1094, CVE-2018-14609

Description

The scan detected that the host is missing the following update:
ELSA-2019-4533

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-February/008476.html

OEL6
x86_64
kernel-uek-2.6.39-400.306.1.el6uek
kernel-uek-devel-2.6.39-400.306.1.el6uek
kernel-uek-doc-2.6.39-400.306.1.el6uek
kernel-uek-debug-devel-2.6.39-400.306.1.el6uek
kernel-uek-debug-2.6.39-400.306.1.el6uek
kernel-uek-firmware-2.6.39-400.306.1.el6uek

i386
kernel-uek-2.6.39-400.306.1.el6uek
kernel-uek-devel-2.6.39-400.306.1.el6uek
kernel-uek-doc-2.6.39-400.306.1.el6uek
kernel-uek-debug-devel-2.6.39-400.306.1.el6uek
kernel-uek-debug-2.6.39-400.306.1.el6uek
kernel-uek-firmware-2.6.39-400.306.1.el6uek

171068 - Amazon Linux AMI ALAS-2019-1151 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-0500, CVE-2018-20483

Description

The scan detected that the host is missing the following update:
ALAS-2019-1151

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1151.html

Amazon Linux AMI
x86_64
curl-7.61.1-7.91.amzn1
curl-debuginfo-7.61.1-7.91.amzn1
libcurl-devel-7.61.1-7.91.amzn1
libcurl-7.61.1-7.91.amzn1

i686
curl-7.61.1-7.91.amzn1
curl-debuginfo-7.61.1-7.91.amzn1
libcurl-devel-7.61.1-7.91.amzn1
libcurl-7.61.1-7.91.amzn1

171069 - Amazon Linux AMI ALAS-2019-1156 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-5736

Description

The scan detected that the host is missing the following update:
ALAS-2019-1156

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1156.html

Amazon Linux AMI
x86_64
docker-18.06.1ce-7.25.amzn1
docker-debuginfo-18.06.1ce-7.25.amzn1

171070 - Amazon Linux AMI ALAS-2019-1150 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-9262

Description

The scan detected that the host is missing the following update:
ALAS-2019-1150

Observation

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

https://alas.aws.amazon.com/ALAS-2019-1150.html

Amazon Linux AMI
x86_64
libXcursor-1.1.14-2.1.10.amzn1
libXcursor-devel-1.1.14-2.1.10.amzn1
libXcursor-debuginfo-1.1.14-2.1.10.amzn1

i686
libXcursor-debuginfo-1.1.14-2.1.10.amzn1
libXcursor-devel-1.1.14-2.1.10.amzn1
libXcursor-1.1.14-2.1.10.amzn1

182908 - FreeBSD curl Multiple Vulnerabilities (714b033a-2b09-11e9-8bc3-610fd6e6cd05)

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

Risk Level: High

CVE: CVE-2018-16890, CVE-2019-3822, CVE-2019-3823

Description

The scan detected that the host is missing the following update:
curl -- multiple vulnerabilities (714b033a-2b09-11e9-8bc3-610fd6e6cd05)

Observation

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

http://www.vuxml.org/freebsd/714b033a-2b09-11e9-8bc3-610fd6e6cd05.html

Affected packages:
curl < 7.64.0

182910 - FreeBSD unit Heap Memory Buffer Overflow (c95836a0-2b3b-11e9-9838-8c164567ca3c)

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

Risk Level: High

CVE: CVE-2019-7401

Description

The scan detected that the host is missing the following update:
unit -- heap memory buffer overflow (c95836a0-2b3b-11e9-9838-8c164567ca3c)

Observation

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

http://www.vuxml.org/freebsd/c95836a0-2b3b-11e9-9838-8c164567ca3c.html

Affected packages:
0.3.0 <= unit < 1.7.1

186568 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3882-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16890, CVE-2019-3822, CVE-2019-3823

Description

The scan detected that the host is missing the following update:
USN-3882-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004763.html

Ubuntu 16.04

libcurl3-nss_7.47.0-1ubuntu2.12
libcurl3-gnutls_7.47.0-1ubuntu2.12
libcurl3_7.47.0-1ubuntu2.12
curl_7.47.0-1ubuntu2.12

Ubuntu 18.10

libcurl3-gnutls_7.61.0-1ubuntu2.3
libcurl4_7.61.0-1ubuntu2.3
curl_7.61.0-1ubuntu2.3
libcurl3-nss_7.61.0-1ubuntu2.3

Ubuntu 14.04

libcurl3-nss_7.35.0-1ubuntu2.20
libcurl3_7.35.0-1ubuntu2.20
curl_7.35.0-1ubuntu2.20
libcurl3-gnutls_7.35.0-1ubuntu2.20

Ubuntu 18.04

curl_7.58.0-2ubuntu3.6
libcurl4_7.58.0-2ubuntu3.6
libcurl3-nss_7.58.0-2ubuntu3.6
libcurl3-gnutls_7.58.0-2ubuntu3.6

186569 - Ubuntu Linux 14.04, 16.04, 18.04 USN-3871-5 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10876, CVE-2018-10877, CVE-2018-10878, CVE-2018-10879, CVE-2018-10880, CVE-2018-10882, CVE-2018-10883, CVE-2018-14625, CVE-2018-16882, CVE-2018-17972, CVE-2018-18281, CVE-2018-19407, CVE-2018-9516

Description

The scan detected that the host is missing the following update:
USN-3871-5

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004766.html

Ubuntu 16.04

linux-image-4.15.0-1037-azure_4.15.0-1037.39~16.04.1
linux-image-azure_4.15.0.1037.42

Ubuntu 14.04

linux-image-4.15.0-1037-azure_4.15.0-1037.39~14.04.2
linux-image-azure_4.15.0.1037.24

Ubuntu 18.04

linux-image-azure_4.15.0.1037.37
linux-image-4.15.0-1037-azure_4.15.0-1037.39

194745 - Fedora Linux 29 FEDORA-2019-077a3f23c0 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-17183, CVE-2018-17961, CVE-2018-18073, CVE-2018-18284, CVE-2018-19134, CVE-2018-19409, CVE-2018-19475, CVE-2018-19476, CVE-2018-19477, CVE-2018-19478

Description

The scan detected that the host is missing the following update:
FEDORA-2019-077a3f23c0

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

ghostscript-9.26-1.fc29

194746 - Fedora Linux 29 FEDORA-2019-76fbe24cab Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6978

Description

The scan detected that the host is missing the following update:
FEDORA-2019-76fbe24cab

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

libwmf-0.2.12-1.fc29

194748 - Fedora Linux 28 FEDORA-2019-f1626b52e9 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-10995, CVE-2019-6438

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f1626b52e9

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=2

Fedora Core 28

slurm-17.11.13-2.fc28

194758 - Fedora Linux 28 FEDORA-2019-6cfd17b03d Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6798, CVE-2019-6799

Description

The scan detected that the host is missing the following update:
FEDORA-2019-6cfd17b03d

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=2

Fedora Core 28

phpMyAdmin-4.8.5-1.fc28

194760 - Fedora Linux 29 FEDORA-2019-ac70292cfc Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-20174, CVE-2018-20175, CVE-2018-20176, CVE-2018-20177, CVE-2018-20178, CVE-2018-20179, CVE-2018-20180, CVE-2018-20181, CVE-2018-20182, CVE-2018-8791, CVE-2018-8792, CVE-2018-8793, CVE-2018-8794, CVE-2018-8795, CVE-2018-8796, CVE-2018-8797, CVE-2018-8798, CVE-2018-8799, CVE-2018-8800

Description

The scan detected that the host is missing the following update:
FEDORA-2019-ac70292cfc

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

rdesktop-1.8.4-2.fc29

194762 - Fedora Linux 28 FEDORA-2019-e9bc354ee8 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6978

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e9bc354ee8

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 28

libwmf-0.2.12-1.fc28

194767 - Fedora Linux 29 FEDORA-2019-43489941ff Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-16839, CVE-2018-16840, CVE-2018-16842, CVE-2018-16890, CVE-2018-20483, CVE-2019-3822, CVE-2019-3823

Description

The scan detected that the host is missing the following update:
FEDORA-2019-43489941ff

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

curl-7.61.1-8.fc29

194769 - Fedora Linux 29 FEDORA-2019-09ae31d880 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-6798, CVE-2019-6799

Description

The scan detected that the host is missing the following update:
FEDORA-2019-09ae31d880

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=2

Fedora Core 29

phpMyAdmin-4.8.5-1.fc29

194772 - Fedora Linux 29 FEDORA-2018-51ce232320 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4463, CVE-2017-12627

Description

The scan detected that the host is missing the following update:
FEDORA-2018-51ce232320

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

xerces-c27-2.7.0-28.fc29

24729 - (MSPT-Feb2019) Microsoft Internet Explorer Information Disclosure Vulnerability (CVE-2019-0676)

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

Risk Level: Medium

CVE: CVE-2019-0676

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to Information Disclosure.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to Information Disclosure.

The flaw lies in the Internet Explorer component. Successful exploitation by a remote attacker could result in Information Disclosure on the target.

24736 - (MSPT-Feb2019) Microsoft Edge Remote Code Execution Vulnerability (CVE-2019-0645)

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

Risk Level: Medium

CVE: CVE-2019-0645

Description

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the improper handling of objects in memory. Successful exploitation by an attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

160514 - CentOS 7 CESA-2019-0229 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16540, CVE-2018-19475, CVE-2018-19476, CVE-2018-19477, CVE-2019-6116

Description

The scan detected that the host is missing the following update:
CESA-2019-0229

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-February/023191.html

CentOS 7
i686
ghostscript-devel-9.07-31.el7_6.9
ghostscript-9.07-31.el7_6.9

noarch
ghostscript-doc-9.07-31.el7_6.9

x86_64
ghostscript-9.07-31.el7_6.9
ghostscript-devel-9.07-31.el7_6.9
ghostscript-gtk-9.07-31.el7_6.9
ghostscript-cups-9.07-31.el7_6.9

186573 - Ubuntu Linux 14.04, 16.04 USN-3883-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10119, CVE-2018-10120, CVE-2018-10583, CVE-2018-11790, CVE-2018-16858

Description

The scan detected that the host is missing the following update:
USN-3883-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004762.html

Ubuntu 14.04

libreoffice-core_4.2.8-0ubuntu5.5

Ubuntu 16.04

libreoffice-core_5.1.6~rc2-0ubuntu1~xenial6

194747 - Fedora Linux 28 FEDORA-2019-a8f918005c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14447

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a8f918005c

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 28

mingw-libconfuse-3.2.2-1.fc28

194749 - Fedora Linux 29 FEDORA-2019-f44f095639 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10851, CVE-2018-14626, CVE-2018-14644, CVE-2018-16855, CVE-2019-3806, CVE-2019-3807

Description

The scan detected that the host is missing the following update:
FEDORA-2019-f44f095639

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

pdns-recursor-4.1.9-1.fc29

194754 - Fedora Linux 29 FEDORA-2019-d7b5e168d1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10779, CVE-2018-17100, CVE-2018-17101, CVE-2019-6128

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d7b5e168d1

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=2

Fedora Core 29

libtiff-4.0.10-2.fc29

194765 - Fedora Linux 29 FEDORA-2019-9ccbbfeae1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14447

Description

The scan detected that the host is missing the following update:
FEDORA-2019-9ccbbfeae1

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

mingw-libconfuse-3.2.2-1.fc29

24673 - (MSPT-Feb2019) Microsoft .NET APIs Spoofing Vulnerability (CVE-2019-0657)

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

Risk Level: Medium

CVE: CVE-2019-0657

Description

A vulnerability in some versions of Microsoft .Net could lead to security bypass.

Observation

A vulnerability in some versions of Microsoft .Net could lead to security bypass.

The flaw lies in the api's component. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions.

24674 - (MSPT-Feb2047) Microsoft Win32k Kernel Information Disclosure (CVE-2019-0628)

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

Risk Level: Medium

CVE: CVE-2019-0628

Description

A vulnerability in some versions of Microsoft Win32k could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Win32k could lead to information disclosure.

The flaw lies in the Win32k component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

24675 - (MSPT-Feb2019) Microsoft Windows Storage Service Elevation of Privilege Vulnerability (CVE-2019-0659)

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

Risk Level: Medium

CVE: CVE-2019-0659

Description

A vulnerability in some versions of Microsoft Storage Service could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Storage Service could lead to privilege escalation.

The flaw is due to improper handling of file operations. Successful exploitation could allow authenticated user to gain elevated privileges.

24676 - (MSPT-Feb2019) Microsoft Windows HID Information Disclosure Vulnerability (CVE-2019-0600)

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

Risk Level: Medium

CVE: CVE-2019-0600

Description

A vulnerability in some versions of Microsoft HID could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft HID could lead to information disclosure.

The flaw is due to improper handling of objects in memory. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the attacker to gain execution on the victim system.

24677 - (MSPT-Feb2019) Microsoft Windows HID Information Disclosure Vulnerability (CVE-2019-0601)

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

Risk Level: Medium

CVE: CVE-2019-0601

Description

A vulnerability in some versions of Microsoft HID could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft HID could lead to information disclosure.

The flaw is due to improper handling of objects in memory. Successful exploitation by an attacker could result in the disclosure of

sensitive information. The exploit requires the attacker to gain execution on the victim system.

24678 - (MSPT-Feb2019) Microsoft Windows Security Feature Bypass Vulnerability (CVE-2019-0627)

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

Risk Level: Medium

CVE: CVE-2019-0627

Description

A vulnerability in some versions of Microsoft Device Guard could lead to security bypass.

Observation

A vulnerability in some versions of Microsoft Device Guard could lead to security bypass.

The flaw is due to improper handling of user mode code integrity policies. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. The exploit requires the attacker to first access the local machine

24680 - (MSPT-Feb2019) Microsoft Windows Security Feature Bypass Vulnerability (CVE-2019-0631)

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

Risk Level: Medium

CVE: CVE-2019-0631

Description

A vulnerability in some versions of Microsoft Windows could lead to security bypass.

Observation

A vulnerability in some versions of Microsoft Windows could lead to security bypass.

The flaw is due to improper handling of user mode code integrity policies. Successful exploitation by an attacker could result in the bypass of intended access restrictions. The exploit requires the attacker to access the local machine.

24681 - (MSPT-Feb2019) Microsoft Windows Security Feature Bypass Vulnerability (CVE-2019-0632)

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

Risk Level: Medium

CVE: CVE-2019-0632

Description

A vulnerability in some versions of Microsoft Windows could lead to security bypass.

Observation

A vulnerability in some versions of Microsoft Windows could lead to security bypass.

The flaw lies in the umci component. Successful exploitation by an attacker could result in the bypass of intended access restrictions. The exploit requires the attacker to access the local machine.

24682 - (MSPT-Feb2019) Microsoft Windows Information Disclosure Vulnerability (CVE-2019-0636)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2019-0636

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw is due to improper disclosing file information in Windows. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

24683 - (MSPT-Feb2019) Microsoft Windows Defender Firewall Security Feature Bypass Vulnerability (CVE-2019-0637)

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

Risk Level: Medium

CVE: CVE-2019-0637

Description

A vulnerability in some versions of Microsoft Windows could lead to security bypass.

Observation

A vulnerability in some versions of Microsoft Windows could lead to security bypass.

The flaw lies in the Defender Firewall. Successful exploitation by an attacker could result in the bypass of intended access restrictions.

24684 - (MSPT-Feb2019) Microsoft Windows Kernel Privilege Escalation (CVE-2019-0656)

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

Risk Level: Medium

CVE: CVE-2019-0656

Description

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

24685 - (MSPT-Feb2019) Microsoft Windows Win32k Privilege Escalation (CVE-2019-0623)

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

Risk Level: Medium

CVE: CVE-2019-0623

Description

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw lies in the Win32k component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

24686 - (MSPT-Feb2019) Microsoft Windows Kernel Information Disclosure (CVE-2019-0621)

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

Risk Level: Medium

CVE: CVE-2019-0621

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the kernel component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

24687 - (MSPT-Feb2019) Microsoft Windows Kernel Information Disclosure (CVE-2019-0661)

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

Risk Level: Medium

CVE: CVE-2019-0661

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the kernel component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

24695 - (MSPT-Feb2019) Microsoft Chakra Improperly Discloses Contents of Memory Information Disclosure (CVE-2019-0648)

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

Risk Level: Medium

CVE: CVE-2019-0648

Description

A vulnerability in some versions of Microsoft Chakra could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Chakra could lead to information disclosure.

The flaw lies in the improperly discloses contents of memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

24696 - (MSPT-Feb2019) Microsoft Chakra JIT server Privilege Escalation (CVE-2019-0649)

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

Risk Level: Medium

CVE: CVE-2019-0649

Description

A vulnerability in some versions of Microsoft Chakra could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Chakra could lead to privilege escalation.

The flaw lies in the JIT server component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

24709 - (MSPT-Feb2019) Microsoft Office Not Validate URLs Security Bypass (CVE-2019-0540)

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

Risk Level: Medium

CVE: CVE-2019-0540

Description

A vulnerability in some versions of Microsoft Office could lead to security bypass.

Observation

A vulnerability in some versions of Microsoft Office could lead to security bypass.

The flaw lies in not validate urls. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. The exploit requires the user to open a vulnerable website, email or document.

24710 - (MSPT-Feb2019) Microsoft Excel Improperly Discloses Contents of Memory Information Disclosure (CVE-2019-0669)

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

Risk Level: Medium

CVE: CVE-2019-0669

Description

A vulnerability in some versions of Microsoft Excel could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Excel could lead to information disclosure.

The flaw lies in the improperly discloses contents of memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

24715 - (MSPT-Feb2019) Microsoft Office Access Connectivity Engine Remote Code Execution (CVE-2019-0675)

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

Risk Level: Medium

CVE: CVE-2019-0675

Description

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

The flaw lies due the access connectivity engine. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

24716 - (MSPT-Feb2019) Microsoft Windows Graphics Device Interface component Information Disclosure (CVE-2019-0660)

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

Risk Level: Medium

CVE: CVE-2019-0660

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the graphics device interface component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

24717 - (MSPT-Feb2019) Microsoft Windows Graphics Device Interface Information Disclosure (CVE-2019-0664)

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

Risk Level: Medium

CVE: CVE-2019-0664

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the graphics device interface component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

24719 - (MSPT-Feb2019) Microsoft Windows GDI Information Disclosure (CVE-2019-0619)

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

Risk Level: Medium

CVE: CVE-2019-0619

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the gdi component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

24721 - (MSPT-Feb2019) Microsoft Windows GDI Information Disclosure (CVE-2019-0616)

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

Risk Level: Medium

CVE: CVE-2019-0616

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the gdi component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

24722 - (MSPT-Feb2019) Microsoft Windows GDI Information Disclosure (CVE-2019-0615)

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

Risk Level: Medium

CVE: CVE-2019-0615

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the gdi component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

24723 - (MSPT-Feb2019) Microsoft Windows GDI Information Disclosure (CVE-2019-0602)

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

Risk Level: Medium

CVE: CVE-2019-0602

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the GDI component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

24728 - (MSPT-Feb2019) Microsoft Browsers Spoofing Vulnerability (CVE-2019-0654)

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

Risk Level: Medium

CVE: CVE-2019-0654

Description

A vulnerability in some versions of Microsoft Browsers could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft Browsers could lead to spoofing.

The flaw lies in Internet Explorer. Successful exploitation by a remote attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

24731 - (MSPT-Feb2019) Microsoft Windows Hyper-V Information Disclosure (CVE-2019-0635)

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

Risk Level: Medium

CVE: CVE-2019-0635

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the Hyper-V component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

24734 - (MSPT-Feb2019) Microsoft Edge Security Feature Bypass Vulnerability (CVE-2019-0641)

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

Risk Level: Medium

CVE: CVE-2019-0641

Description

A vulnerability in some versions of Microsoft Edge could lead to security bypass.

Observation

A vulnerability in some versions of Microsoft Edge could lead to security bypass.

The flaw lies in the improper handling of whitelisting in edgehtmlpluginpolicy component. Successful exploitation by a remote attacker

could result in the bypass of intended access restrictions.

24735 - (MSPT-Feb2019) Microsoft Edge Information Disclosure Vulnerability (CVE-2019-0643)

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

Risk Level: Medium

CVE: CVE-2019-0643

Description

A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

The flaw is due to improper handling of cross-origin requests. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

24737 - (MSPT-Feb2019) Microsoft Edge Information Disclosure Vulnerability (CVE-2019-0658)

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

Risk Level: Medium

CVE: CVE-2019-0658

Description

A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Edge could lead to information disclosure.

The flaw is in the Microsoft Scripting Engine Component. Successful exploitation by an attacker could result in the disclosure of sensitive information.

24738 - (MSPT-Feb2019) Microsoft Windows Server DHCP Information Disclosure (CVE-2019-0626)

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

Risk Level: Medium

CVE: CVE-2019-0626

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the Server dhcp component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

24741 - (MSPT-Feb2019) Microsoft SharePoint Improperly Sanitize Web Request Privilege Escalation (CVE-2019-0668)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2019-0668

Description

A vulnerability in some versions of Microsoft SharePoint could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft SharePoint could lead to privilege escalation.

The flaw lies due the improperly sanitize web request. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

24742 - (MSPT-Feb2019) Microsoft SharePoint Improperly Parse HTTP Content Spoofing (CVE-2019-0670)

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

Risk Level: Medium

CVE: CVE-2019-0670

Description

A vulnerability in some versions of Microsoft SharePoint could lead to spoofing.

Observation

A vulnerability in some versions of Microsoft SharePoint could lead to spoofing.

The flaw lies due the improperly parse http content. Successful exploitation by a remote attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

24764 - (MSPT-Feb2019) Microsoft Exchange Server Privilege Escalation (CVE-2019-0686)

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

Risk Level: Medium

CVE: CVE-2019-0686

Description

A vulnerability in some versions of Microsoft Exchange could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Exchange could lead to privilege escalation.

The flaw lies in the authentication request component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

24765 - (MSPT-Feb2019) Microsoft Exchange Server Privilege Escalation (CVE-2019-0724)

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

Risk Level: Medium

CVE: CVE-2019-0724

Description

A vulnerability in some versions of Microsoft Exchange could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Exchange could lead to privilege escalation.

The flaw lies in the authentication request component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

147606 - SuSE Linux 15.0 openSUSE-SU-2019:0153-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11803

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0153-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00041.html

SuSE Linux 15.0
i586
subversion-devel-1.10.0-lp150.2.3.1
subversion-ruby-1.10.0-lp150.2.3.1
subversion-server-debuginfo-1.10.0-lp150.2.3.1
subversion-perl-1.10.0-lp150.2.3.1
libsvn_auth_gnome_keyring-1-0-1.10.0-lp150.2.3.1
libsvn_auth_kwallet-1-0-debuginfo-1.10.0-lp150.2.3.1
subversion-ruby-debuginfo-1.10.0-lp150.2.3.1
subversion-python-debuginfo-1.10.0-lp150.2.3.1
subversion-debugsource-1.10.0-lp150.2.3.1
subversion-tools-1.10.0-lp150.2.3.1
libsvn_auth_gnome_keyring-1-0-debuginfo-1.10.0-lp150.2.3.1
subversion-server-1.10.0-lp150.2.3.1
subversion-perl-debuginfo-1.10.0-lp150.2.3.1
libsvn_auth_kwallet-1-0-1.10.0-lp150.2.3.1
subversion-tools-debuginfo-1.10.0-lp150.2.3.1
subversion-debuginfo-1.10.0-lp150.2.3.1
subversion-python-ctypes-1.10.0-lp150.2.3.1
subversion-1.10.0-lp150.2.3.1
subversion-python-1.10.0-lp150.2.3.1

noarch
subversion-bash-completion-1.10.0-lp150.2.3.1

x86_64
subversion-devel-1.10.0-lp150.2.3.1
subversion-ruby-1.10.0-lp150.2.3.1
subversion-server-debuginfo-1.10.0-lp150.2.3.1
subversion-perl-1.10.0-lp150.2.3.1
libsvn_auth_gnome_keyring-1-0-1.10.0-lp150.2.3.1
libsvn_auth_kwallet-1-0-debuginfo-1.10.0-lp150.2.3.1
subversion-ruby-debuginfo-1.10.0-lp150.2.3.1

subversion-python-debuginfo-1.10.0-lp150.2.3.1
subversion-debugsource-1.10.0-lp150.2.3.1
subversion-tools-1.10.0-lp150.2.3.1
libsvn_auth_gnome_keyring-1-0-debuginfo-1.10.0-lp150.2.3.1
subversion-server-1.10.0-lp150.2.3.1
subversion-perl-debuginfo-1.10.0-lp150.2.3.1
libsvn_auth_kwallet-1-0-1.10.0-lp150.2.3.1
subversion-tools-debuginfo-1.10.0-lp150.2.3.1
subversion-debuginfo-1.10.0-lp150.2.3.1
subversion-python-ctypes-1.10.0-lp150.2.3.1
subversion-1.10.0-lp150.2.3.1
subversion-python-1.10.0-lp150.2.3.1

147612 - SuSE Linux 15.0 openSUSE-SU-2019:0155-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20406, CVE-2019-5010

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0155-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00045.html

SuSE Linux 15.0
i586
python3-dbm-3.6.5-lp150.2.6.1
python3-tk-debuginfo-3.6.5-lp150.2.6.1
python3-base-debuginfo-3.6.5-lp150.2.6.1
python3-tools-3.6.5-lp150.2.6.1
python3-tk-3.6.5-lp150.2.6.1
python3-testsuite-debuginfo-3.6.5-lp150.2.6.1
python3-base-debugsource-3.6.5-lp150.2.6.1
python3-debugsource-3.6.5-lp150.2.6.1
python3-devel-3.6.5-lp150.2.6.1
python3-testsuite-3.6.5-lp150.2.6.1
python3-debuginfo-3.6.5-lp150.2.6.1
python3-curses-3.6.5-lp150.2.6.1
python3-idle-3.6.5-lp150.2.6.1
python3-3.6.5-lp150.2.6.1
python3-devel-debuginfo-3.6.5-lp150.2.6.1
libpython3_6m1_0-debuginfo-3.6.5-lp150.2.6.1
python3-base-3.6.5-lp150.2.6.1
python3-dbm-debuginfo-3.6.5-lp150.2.6.1
python3-curses-debuginfo-3.6.5-lp150.2.6.1
libpython3_6m1_0-3.6.5-lp150.2.6.1

noarch
python3-doc-3.6.5-lp150.2.6.1

x86_64
python3-dbm-3.6.5-lp150.2.6.1
python3-tk-debuginfo-3.6.5-lp150.2.6.1

libpython3_6m1_0-32bit-3.6.5-lp150.2.6.1
python3-base-debuginfo-3.6.5-lp150.2.6.1
python3-tools-3.6.5-lp150.2.6.1
python3-tk-3.6.5-lp150.2.6.1
python3-testsuite-debuginfo-3.6.5-lp150.2.6.1
python3-base-debugsource-3.6.5-lp150.2.6.1
python3-32bit-debuginfo-3.6.5-lp150.2.6.1
python3-base-32bit-debuginfo-3.6.5-lp150.2.6.1
python3-debugsource-3.6.5-lp150.2.6.1
python3-devel-3.6.5-lp150.2.6.1
python3-testsuite-3.6.5-lp150.2.6.1
python3-32bit-3.6.5-lp150.2.6.1
python3-debuginfo-3.6.5-lp150.2.6.1
libpython3_6m1_0-32bit-debuginfo-3.6.5-lp150.2.6.1
python3-curses-3.6.5-lp150.2.6.1
python3-idle-3.6.5-lp150.2.6.1
python3-3.6.5-lp150.2.6.1
python3-devel-debuginfo-3.6.5-lp150.2.6.1
python3-base-32bit-3.6.5-lp150.2.6.1
libpython3_6m1_0-debuginfo-3.6.5-lp150.2.6.1
python3-base-3.6.5-lp150.2.6.1
python3-dbm-debuginfo-3.6.5-lp150.2.6.1
python3-curses-debuginfo-3.6.5-lp150.2.6.1
libpython3_6m1_0-3.6.5-lp150.2.6.1

147616 - SuSE Linux 42.3 openSUSE-SU-2019:0154-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-16881

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0154-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00043.html

SuSE Linux 42.3
x86_64
rsyslog-module-omamqp1-debuginfo-8.24.0-2.10.1
rsyslog-module-pgsql-debuginfo-8.24.0-2.10.1
rsyslog-diag-tools-debuginfo-8.24.0-2.10.1
rsyslog-module-omtcl-debuginfo-8.24.0-2.10.1
rsyslog-module-guardtime-8.24.0-2.10.1
rsyslog-module-gtls-debuginfo-8.24.0-2.10.1
rsyslog-module-gssapi-8.24.0-2.10.1
rsyslog-module-relp-8.24.0-2.10.1
rsyslog-debugsource-8.24.0-2.10.1
rsyslog-module-mmnormalize-debuginfo-8.24.0-2.10.1
rsyslog-module-mysql-8.24.0-2.10.1
rsyslog-debuginfo-8.24.0-2.10.1
rsyslog-module-dbi-8.24.0-2.10.1
rsyslog-module-udpspoof-debuginfo-8.24.0-2.10.1
rsyslog-module-udpspoof-8.24.0-2.10.1

rsyslog-diag-tools-8.24.0-2.10.1
rsyslog-module-dbi-debuginfo-8.24.0-2.10.1
rsyslog-module-elasticsearch-8.24.0-2.10.1
rsyslog-module-mmnormalize-8.24.0-2.10.1
rsyslog-module-omhttpfs-debuginfo-8.24.0-2.10.1
rsyslog-8.24.0-2.10.1
rsyslog-doc-8.24.0-2.10.1
rsyslog-module-relp-debuginfo-8.24.0-2.10.1
rsyslog-module-snmp-8.24.0-2.10.1
rsyslog-module-omhttpfs-8.24.0-2.10.1
rsyslog-module-gcrypt-debuginfo-8.24.0-2.10.1
rsyslog-module-omtcl-8.24.0-2.10.1
rsyslog-module-pgsql-8.24.0-2.10.1
rsyslog-module-elasticsearch-debuginfo-8.24.0-2.10.1
rsyslog-module-gssapi-debuginfo-8.24.0-2.10.1
rsyslog-module-gcrypt-8.24.0-2.10.1
rsyslog-module-guardtime-debuginfo-8.24.0-2.10.1
rsyslog-module-omamqp1-8.24.0-2.10.1
rsyslog-module-mysql-debuginfo-8.24.0-2.10.1
rsyslog-module-gtls-8.24.0-2.10.1
rsyslog-module-snmp-debuginfo-8.24.0-2.10.1

i586
rsyslog-module-omamqp1-debuginfo-8.24.0-2.10.1
rsyslog-module-pgsql-debuginfo-8.24.0-2.10.1
rsyslog-diag-tools-debuginfo-8.24.0-2.10.1
rsyslog-module-omtcl-debuginfo-8.24.0-2.10.1
rsyslog-module-guardtime-8.24.0-2.10.1
rsyslog-module-gtls-debuginfo-8.24.0-2.10.1
rsyslog-module-gssapi-8.24.0-2.10.1
rsyslog-module-relp-8.24.0-2.10.1
rsyslog-debugsource-8.24.0-2.10.1
rsyslog-module-mmnormalize-debuginfo-8.24.0-2.10.1
rsyslog-module-mysql-8.24.0-2.10.1
rsyslog-debuginfo-8.24.0-2.10.1
rsyslog-module-dbi-8.24.0-2.10.1
rsyslog-module-udpspoof-debuginfo-8.24.0-2.10.1
rsyslog-module-udpspoof-8.24.0-2.10.1
rsyslog-diag-tools-8.24.0-2.10.1
rsyslog-module-dbi-debuginfo-8.24.0-2.10.1
rsyslog-module-elasticsearch-8.24.0-2.10.1
rsyslog-module-mmnormalize-8.24.0-2.10.1
rsyslog-module-omhttpfs-debuginfo-8.24.0-2.10.1
rsyslog-8.24.0-2.10.1
rsyslog-doc-8.24.0-2.10.1
rsyslog-module-relp-debuginfo-8.24.0-2.10.1
rsyslog-module-snmp-8.24.0-2.10.1
rsyslog-module-omhttpfs-8.24.0-2.10.1
rsyslog-module-gcrypt-debuginfo-8.24.0-2.10.1
rsyslog-module-omtcl-8.24.0-2.10.1
rsyslog-module-pgsql-8.24.0-2.10.1
rsyslog-module-elasticsearch-debuginfo-8.24.0-2.10.1
rsyslog-module-gssapi-debuginfo-8.24.0-2.10.1
rsyslog-module-gcrypt-8.24.0-2.10.1
rsyslog-module-guardtime-debuginfo-8.24.0-2.10.1
rsyslog-module-omamqp1-8.24.0-2.10.1
rsyslog-module-mysql-debuginfo-8.24.0-2.10.1
rsyslog-module-gtls-8.24.0-2.10.1
rsyslog-module-snmp-debuginfo-8.24.0-2.10.1

147622 - SuSE SLES 11 SP4 SUSE-SU-2019:13943-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3813

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13943-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005094.html

SuSE SLES 11 SP4
x86_64
libspice-server1-0.12.4-18.1

i586
libspice-server1-0.12.4-18.1

160517 - CentOS 7 CESA-2019-0231 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3813

Description

The scan detected that the host is missing the following update:
CESA-2019-0231

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-February/023192.html

CentOS 7
x86_64
spice-server-0.14.0-6.el7_6.1
spice-server-devel-0.14.0-6.el7_6.1

160518 - CentOS 6 CESA-2019-0232 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3813

Description

The scan detected that the host is missing the following update:
CESA-2019-0232

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-February/023189.html

CentOS 6
x86_64
spice-server-0.12.4-16.el6_10.3
spice-server-devel-0.12.4-16.el6_10.3

194750 - Fedora Linux 29 FEDORA-2019-7e722314f3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-7313

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7e722314f3

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

buildbot-1.8.1-1.fc29

194752 - Fedora Linux 29 FEDORA-2019-a095a16c47 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-3813

Description

The scan detected that the host is missing the following update:
FEDORA-2019-a095a16c47

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

spice-0.14.1-2.fc29

194761 - Fedora Linux 28 FEDORA-2019-cf9ddf9fff Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10583, CVE-2018-16858

Description

The scan detected that the host is missing the following update:
FEDORA-2019-cf9ddf9fff

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=3

Fedora Core 28

libreoffice-6.0.7.3-1.fc28

194773 - Fedora Linux 28 FEDORA-2019-7eb8c71fe8 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2019-7313

Description

The scan detected that the host is missing the following update:
FEDORA-2019-7eb8c71fe8

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 28

buildbot-1.8.1-1.fc28

131295 - Debian Linux 9.0 DSA-4387-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
DSA-4387-1

Observation

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

http://www.debian.org/security/2019/dsa-4387

Debian 9.0
all

openssh-server-udeb_1:7.4p1-10+deb9u5
openssh-client-udeb_1:7.4p1-10+deb9u5
ssh_1:7.4p1-10+deb9u5
ssh-askpass-gnome_1:7.4p1-10+deb9u5
openssh-server_1:7.4p1-10+deb9u5
openssh-sftp-server_1:7.4p1-10+deb9u5
openssh-client-ssh1_1:7.4p1-10+deb9u5
ssh-krb5_1:7.4p1-10+deb9u5
openssh-client_1:7.4p1-10+deb9u5

132496 - Oracle VM OVMSA-2019-0007 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12153, CVE-2018-17972, CVE-2018-3639

Description

The scan detected that the host is missing the following update:
OVMSA-2019-0007

Observation

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

http://oss.oracle.com/pipermail/oraclevm-errata/2019-February/000928.html

OVM3.4
x86_64
kernel-uek-4.1.12-124.25.1.el6uek
kernel-uek-firmware-4.1.12-124.25.1.el6uek

147609 - SuSE Linux 15.0 openSUSE-SU-2019:0152-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-0737

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0152-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00039.html

SuSE Linux 15.0
i586
libopenssl1_1-1.1.0i-lp150.3.18.1
openssl-1_1-1.1.0i-lp150.3.18.1
libopenssl-1_1-devel-1.1.0i-lp150.3.18.1
libopenssl1_1-debuginfo-1.1.0i-lp150.3.18.1
openssl-1_1-debuginfo-1.1.0i-lp150.3.18.1
libopenssl1_1-hmac-1.1.0i-lp150.3.18.1
openssl-1_1-debugsource-1.1.0i-lp150.3.18.1

noarch
openssl-1_1-doc-1.1.0i-lp150.3.18.1

x86_64
libopenssl1_1-1.1.0i-lp150.3.18.1
openssl-1_1-1.1.0i-lp150.3.18.1
libopenssl-1_1-devel-1.1.0i-lp150.3.18.1
libopenssl-1_1-devel-32bit-1.1.0i-lp150.3.18.1
libopenssl1_1-debuginfo-1.1.0i-lp150.3.18.1
openssl-1_1-debuginfo-1.1.0i-lp150.3.18.1
libopenssl1_1-32bit-1.1.0i-lp150.3.18.1
libopenssl1_1-hmac-32bit-1.1.0i-lp150.3.18.1
libopenssl1_1-hmac-1.1.0i-lp150.3.18.1
libopenssl1_1-32bit-debuginfo-1.1.0i-lp150.3.18.1
openssl-1_1-debugsource-1.1.0i-lp150.3.18.1

147618 - SuSE Linux 15.0 openSUSE-SU-2019:0161-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11212, CVE-2019-2422, CVE-2019-2426

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0161-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00047.html

SuSE Linux 15.0
x86_64
java-11-openjdk-debuginfo-11.0.2.0-lp150.2.12.1
java-11-openjdk-devel-11.0.2.0-lp150.2.12.1
java-11-openjdk-11.0.2.0-lp150.2.12.1
java-11-openjdk-demo-11.0.2.0-lp150.2.12.1
java-11-openjdk-debugsource-11.0.2.0-lp150.2.12.1
java-11-openjdk-accessibility-11.0.2.0-lp150.2.12.1
java-11-openjdk-headless-11.0.2.0-lp150.2.12.1
java-11-openjdk-accessibility-debuginfo-11.0.2.0-lp150.2.12.1
java-11-openjdk-src-11.0.2.0-lp150.2.12.1
java-11-openjdk-jmods-11.0.2.0-lp150.2.12.1

noarch
java-11-openjdk-javadoc-11.0.2.0-lp150.2.12.1

147623 - SuSE SLES 11 SP4 SUSE-SU-2019:13948-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-10906

Description

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

SUSE-SU-2019:13948-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005097.html

SuSE SLES 11 SP4
i586
libfuse2-2.8.7-0.11.3.1
fuse-2.8.7-0.11.3.1

x86_64
libfuse2-2.8.7-0.11.3.1
fuse-2.8.7-0.11.3.1

163804 - Oracle Enterprise Linux ELSA-2019-4541 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-13053, CVE-2018-16882, CVE-2018-17972, CVE-2018-18397, CVE-2019-5489

Description

The scan detected that the host is missing the following update:
ELSA-2019-4541

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-February/008486.html

OEL7
x86_64
kernel-uek-doc-4.14.35-1844.2.5.el7uek
kernel-uek-devel-4.14.35-1844.2.5.el7uek
kernel-uek-debug-4.14.35-1844.2.5.el7uek
kernel-uek-debug-devel-4.14.35-1844.2.5.el7uek
kernel-uek-tools-4.14.35-1844.2.5.el7uek
kernel-uek-4.14.35-1844.2.5.el7uek

163806 - Oracle Enterprise Linux ELSA-2019-4531 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12153, CVE-2018-17972, CVE-2018-3639

Description

The scan detected that the host is missing the following update:
ELSA-2019-4531

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-February/008472.html
http://oss.oracle.com/pipermail/el-errata/2019-February/008473.html

OEL7
x86_64
kernel-uek-debug-4.1.12-124.25.1.el7uek
kernel-uek-doc-4.1.12-124.25.1.el7uek
kernel-uek-debug-devel-4.1.12-124.25.1.el7uek
kernel-uek-firmware-4.1.12-124.25.1.el7uek
kernel-uek-4.1.12-124.25.1.el7uek
kernel-uek-devel-4.1.12-124.25.1.el7uek

OEL6
x86_64
kernel-uek-debug-devel-4.1.12-124.25.1.el6uek
kernel-uek-4.1.12-124.25.1.el6uek
kernel-uek-devel-4.1.12-124.25.1.el6uek
kernel-uek-debug-4.1.12-124.25.1.el6uek
kernel-uek-firmware-4.1.12-124.25.1.el6uek
kernel-uek-doc-4.1.12-124.25.1.el6uek

182911 - FreeBSD OpenJPEG Integer Overflow (5efd7a93-2dfb-11e9-9549-e980e869c2e9)

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

Risk Level: Medium

CVE: CVE-2018-5727

Description

The scan detected that the host is missing the following update:
OpenJPEG -- integer overflow (5efd7a93-2dfb-11e9-9549-e980e869c2e9)

Observation

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

http://www.vuxml.org/freebsd/5efd7a93-2dfb-11e9-9549-e980e869c2e9.html

Affected packages:
openjpeg <= 2.3.0_3

186570 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3885-1 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
USN-3885-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004765.html

Ubuntu 16.04

openssh-client_7.2p2-4ubuntu2.7

Ubuntu 18.10

openssh-client_7.7p1-4ubuntu0.2

Ubuntu 14.04

openssh-client_6.6p1-2ubuntu2.12

Ubuntu 18.04

openssh-client_7.6p1-4ubuntu0.2

186572 - Ubuntu Linux 18.10 USN-3878-2 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-14625, CVE-2018-16882, CVE-2018-19407, CVE-2018-19854

Description

The scan detected that the host is missing the following update:
USN-3878-2

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004767.html

Ubuntu 18.10

linux-image-4.18.0-1008-azure_4.18.0-1008.8
linux-image-azure_4.18.0.1008.9

194755 - Fedora Linux 29 FEDORA-2018-b89746cb9b Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11784

Description

The scan detected that the host is missing the following update:
FEDORA-2018-b89746cb9b

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

tomcat-9.0.13-1.fc29

194766 - Fedora Linux 29 FEDORA-2019-8f2b27efce Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-3639

Description

The scan detected that the host is missing the following update:
FEDORA-2019-8f2b27efce

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

java-1.8.0-openjdk-1.8.0.201.b09-2.fc29

194771 - Fedora Linux 28 FEDORA-2019-40f4af0687 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-18267, CVE-2018-13988, CVE-2018-18897, CVE-2018-20481, CVE-2018-20551, CVE-2018-20650

Description

The scan detected that the host is missing the following update:
FEDORA-2019-40f4af0687

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=3

Fedora Core 28

poppler-0.62.0-14.fc28

89001 - Slackware Linux 14.0, 14.1, 14.2 SSA:2019-038-01 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:2019-038-01

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=2019&m=slackware-security.489648

Slackware 14.0
x86_64
php-5.6.40-x86_64-1

Slackware 14.2
x86_64
php-5.6.40-x86_64-1

i586
php-5.6.40-i586-1

Slackware 14.1
x86_64
php-5.6.40-x86_64-1

89003 - Slackware Linux 14.2 SSA:2019-043-01 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:2019-043-01

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=2019&m=slackware-security.394423

Slackware 14.2
x86_64
lxc-2.0.9_d3a03247-x86_64-1

i586
lxc-2.0.9_d3a03247-i586-1

131291 - Debian Linux 9.0 DSA-4385-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-3814

Description

The scan detected that the host is missing the following update:
DSA-4385-1

Observation

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

http://www.debian.org/security/2019/dsa-4385

Debian 9.0
all
dovecot-core_1:2.2.27-3+deb9u3
dovecot-lmtpd_1:2.2.27-3+deb9u3
dovecot-ldap_1:2.2.27-3+deb9u3
dovecot-dbg_1:2.2.27-3+deb9u3
dovecot-dev_1:2.2.27-3+deb9u3
dovecot-managesieved_1:2.2.27-3+deb9u3
dovecot-lucene_1:2.2.27-3+deb9u3
dovecot-imapd_1:2.2.27-3+deb9u3
dovecot-pop3d_1:2.2.27-3+deb9u3
dovecot-sqlite_1:2.2.27-3+deb9u3
dovecot-sieve_1:2.2.27-3+deb9u3
dovecot-mysql_1:2.2.27-3+deb9u3
dovecot-gssapi_1:2.2.27-3+deb9u3
dovecot-solr_1:2.2.27-3+deb9u3
dovecot-pgsql_1:2.2.27-3+deb9u3

131292 - Debian Linux 9.0 DSA-4388-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-12546, CVE-2018-12550, CVE-2018-12551

Description

The scan detected that the host is missing the following update:
DSA-4388-1

Observation

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

http://www.debian.org/security/2019/dsa-4388

Debian 9.0
all
mosquitto_1.4.10-3+deb9u3

131293 - Debian Linux 9.0 DSA-4389-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20340

Description

The scan detected that the host is missing the following update:
DSA-4389-1

Observation

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

http://www.debian.org/security/2019/dsa-4389

Debian 9.0
all
u2f-host_1.1.2-2+deb9u1
libu2f-host-dev_1.1.2-2+deb9u1
libu2f-host0_1.1.2-2+deb9u1

147617 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0284-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2015-3239

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0284-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-February/005095.html

SuSE SLED 12 SP3
x86_64
libunwind-debugsource-1.1-11.3.1
libunwind-debuginfo-1.1-11.3.1
libunwind-1.1-11.3.1

SuSE SLED 12 SP4
x86_64
libunwind-debugsource-1.1-11.3.1
libunwind-debuginfo-1.1-11.3.1
libunwind-1.1-11.3.1

SuSE SLES 12 SP4
x86_64
libunwind-devel-1.1-11.3.1
libunwind-debugsource-1.1-11.3.1
libunwind-debuginfo-1.1-11.3.1
libunwind-1.1-11.3.1

SuSE SLES 12 SP3
x86_64
libunwind-devel-1.1-11.3.1
libunwind-debugsource-1.1-11.3.1
libunwind-debuginfo-1.1-11.3.1
libunwind-1.1-11.3.1

182907 - FreeBSD Gitlab Multiple Vulnerabilities (43ee6c1d-29ee-11e9-82a1-001b217b3468)

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

Risk Level: Low

CVE: CVE-2019-6796, CVE-2019-7353

Description

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

Gitlab -- Multiple vulnerabilities (43ee6c1d-29ee-11e9-82a1-001b217b3468)

Observation

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

http://www.vuxml.org/freebsd/43ee6c1d-29ee-11e9-82a1-001b217b3468.html

Affected packages:
11.7.0 <= gitlab-ce < 11.7.4
11.6.0 <= gitlab-ce < 11.6.9

182909 - FreeBSD kf5-kauth Insecure Handling Of Arguments In Helpers (e8bcac84-2d5c-11e9-9a74-e0d55e2a8bf9)

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

Risk Level: Low

CVE: CVE-2019-7443

Description

The scan detected that the host is missing the following update:
kf5-kauth -- Insecure handling of arguments in helpers (e8bcac84-2d5c-11e9-9a74-e0d55e2a8bf9)

Observation

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

http://www.vuxml.org/freebsd/e8bcac84-2d5c-11e9-9a74-e0d55e2a8bf9.html

Affected packages:
kf5-kauth < 5.54.0_2

182912 - FreeBSD FreeBSD File Description Reference Count Leak (86c89abf-2d91-11e9-bf3e-a4badb2f4699)

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

Risk Level: Low

CVE: CVE-2019-5596

Description

The scan detected that the host is missing the following update:
FreeBSD -- File description reference count leak (86c89abf-2d91-11e9-bf3e-a4badb2f4699)

Observation

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

http://www.vuxml.org/freebsd/86c89abf-2d91-11e9-bf3e-a4badb2f4699.html

Affected packages:
12.0 <= FreeBSD-kernel < 12.0_3

182913 - FreeBSD Flash Player Information Disclosure (de11a8fb-2eda-11e9-8fb5-6451062f0f7a)

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

Risk Level: Low

CVE: CVE-2019-7090

Description

The scan detected that the host is missing the following update:
Flash Player -- information disclosure (de11a8fb-2eda-11e9-8fb5-6451062f0f7a)

Observation

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

http://www.vuxml.org/freebsd/de11a8fb-2eda-11e9-8fb5-6451062f0f7a.html

Affected packages:
linux-flashplayer < 32.0.0.142

182914 - FreeBSD FreeBSD System Call Kernel Data Register Leak (683c714d-2d91-11e9-bf3e-a4badb2f4699)

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

Risk Level: Low

CVE: CVE-2019-5595

Description

The scan detected that the host is missing the following update:
FreeBSD -- System call kernel data register leak (683c714d-2d91-11e9-bf3e-a4badb2f4699)

Observation

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

http://www.vuxml.org/freebsd/683c714d-2d91-11e9-bf3e-a4badb2f4699.html

Affected packages:
12.0 <= FreeBSD-kernel < 12.0_3
11.2 <= FreeBSD-kernel < 11.2_9

186571 - Ubuntu Linux 14.04, 16.04, 18.04, 18.10 USN-3887-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-7304

Description

The scan detected that the host is missing the following update:
USN-3887-1

Observation

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

https://lists.ubuntu.com/archives/ubuntu-security-announce/2019-February/004769.html

Ubuntu 16.04

snapd_2.34.2ubuntu0.1

Ubuntu 18.10

snapd_2.35.5+18.10.1

Ubuntu 14.04

snapd_2.34.2~14.04.1

Ubuntu 18.04

snapd_2.34.2+18.04.1

194751 - Fedora Linux 29 FEDORA-2019-fd9345f44a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-5736

Description

The scan detected that the host is missing the following update:
FEDORA-2019-fd9345f44a

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

flatpak-1.2.3-1.fc29

194756 - Fedora Linux 28 FEDORA-2019-333a7aa511 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-333a7aa511

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 28

radvd-2.17-12.fc28

194757 - Fedora Linux 29 FEDORA-2019-e66b1889ec Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-e66b1889ec

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

slurm-17.11.13-2.fc29

194759 - Fedora Linux 28 FEDORA-2019-0c1be924df Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-0c1be924df

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=3

Fedora Core 28

gvfs-1.36.2-3.fc28

194763 - Fedora Linux 29 FEDORA-2019-526ef126cd Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-526ef126cd

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

thunderbird-60.5.0-4.fc29

194764 - Fedora Linux 28 FEDORA-2019-96ac060af3 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
FEDORA-2019-96ac060af3

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=2

Fedora Core 28

java-11-openjdk-11.0.2.7-0.fc28

194770 - Fedora Linux 29 FEDORA-2019-73cbc02e14 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-18898

Description

The scan detected that the host is missing the following update:
FEDORA-2019-73cbc02e14

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

perl-Email-Address-List-0.06-1.fc29

147607 - SuSE Linux 42.3 openSUSE-SU-2019:0159-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-9015

Description

The scan detected that the host is missing the following update:
openSUSE-SU-2019:0159-1

Observation

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

https://lists.opensuse.org/opensuse-updates/2019-02/msg00048.html

SuSE Linux 42.3
noarch
python-urllib3-1.22-4.4.1
python3-urllib3-1.22-4.4.1

194768 - Fedora Linux 29 FEDORA-2019-335c3ad86a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2019-7317

Description

The scan detected that the host is missing the following update:
FEDORA-2019-335c3ad86a

Observation

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

https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/2019/2/?count=200&page=1

Fedora Core 29

libpng-1.6.34-7.fc29

ENHANCED CHECKS

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

88994 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-355-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1160

Update Details

Risk is updated

131261 - Debian Linux 9.0 DSA-4356-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1160

Update Details

Risk is updated

147480 - SuSE SLED 12 SP3, 12 SP4 SUSE-SU-2018:4217-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1160

Update Details

Risk is updated

147510 - SuSE Linux 42.3 openSUSE-SU-2018:4287-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-1160

Update Details

Risk is updated

182899 - FreeBSD mozilla Multiple Vulnerabilities (b1f7d52f-fc42-48e8-8403-87d4c9d26229)

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

Risk Level: High

CVE: CVE-2018-18500, CVE-2018-18501, CVE-2018-18502, CVE-2018-18503, CVE-2018-18504, CVE-2018-18505, CVE-2018-18506

Update Details

Risk is updated

89000 - Slackware Linux 14.2 SSA:2019-029-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Update Details

Risk is updated

131283 - Debian Linux 9.0 DSA-4382-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2019-3463, CVE-2019-3464

Update Details

Risk is updated

131285 - Debian Linux 9.0 DSA-4376-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Update Details

Risk is updated

160508 - CentOS 6 CESA-2019-0218 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Update Details
Risk is updated

160509 - CentOS 7 CESA-2019-0219 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Update Details
Risk is updated

163801 - Oracle Enterprise Linux ELSA-2019-0219 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Update Details
Risk is updated

163802 - Oracle Enterprise Linux ELSA-2019-0218 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Update Details
Risk is updated

182752 - FreeBSD OpenJPEG Multiple Vulnerabilities (11dc3890-0e64-11e8-99b0-d017c2987f9a)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2017-17479, CVE-2017-17480, CVE-2018-5727, CVE-2018-5785, CVE-2018-6616

Update Details
FASLScript is updated

196245 - Red Hat Enterprise Linux RHSA-2019-0219 Update Is Not Installed

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

CVE: CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Update Details

Risk is updated

196248 - Red Hat Enterprise Linux RHSA-2019-0218 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18500, CVE-2018-18501, CVE-2018-18505

Update Details

Risk is updated

131289 - Debian Linux 9.0 DSA-4378-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000888

Update Details

Risk is updated

186529 - Ubuntu Linux 16.04, 18.04, 18.10 USN-3857-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000888

Update Details

Risk is updated

194622 - Fedora Linux 29 FEDORA-2018-1bd545ef39 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20167

Update Details

Risk is updated

194623 - Fedora Linux 28 FEDORA-2018-27f957ae8e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20167

Update Details

Risk is updated

23919 - (JSA10875) Juniper SRX Series ISC BIND Named Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: Medium
CVE: CVE-2017-3138, CVE-2017-3142, CVE-2017-3143, CVE-2017-3145

Update Details
Risk is updated

88858 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-103-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Update Details
Risk is updated

88909 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2018-017-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3145

Update Details
Risk is updated

88919 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2018-060-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

130765 - Debian Linux 8.0 DSA-3854-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Update Details
Risk is updated

130993 - Debian Linux 8.0, 9.0 DSA-4089-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3145

Update Details

Risk is updated

131042 - Debian Linux 8.0, 9.0 DSA-4133-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3144, CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

132430 - Oracle VM OVMSA-2018-0014 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3145

Update Details
Risk is updated

132439 - Oracle VM OVMSA-2018-0024 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

132440 - Oracle VM OVMSA-2018-0023 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

132477 - Oracle VM OVMSA-2018-0252 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle VM Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3142, CVE-2017-3143, CVE-2017-3145, CVE-2018-5740

Update Details
Risk is updated

141555 - Red Hat Enterprise Linux RHSA-2017-1095 Update Is Not Installed

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

CVE: CVE-2017-3136, CVE-2017-3137

Update Details

Risk is updated

141560 - Red Hat Enterprise Linux RHSA-2017-1105 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3136, CVE-2017-3137

Update Details

Risk is updated

141616 - Red Hat Enterprise Linux RHSA-2017-1582 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3137, CVE-2017-3139

Update Details

Risk is updated

141840 - Red Hat Enterprise Linux RHSA-2018-0101 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3145

Update Details

Risk is updated

141842 - Red Hat Enterprise Linux RHSA-2018-0102 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3145

Update Details

Risk is updated

141887 - Red Hat Enterprise Linux RHSA-2018-0488 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3145

Update Details

Risk is updated

141893 - Red Hat Enterprise Linux RHSA-2018-0469 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

141897 - Red Hat Enterprise Linux RHSA-2018-0483 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

141898 - Red Hat Enterprise Linux RHSA-2018-0487 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3145

Update Details
Risk is updated

146311 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0303-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3145

Update Details
Risk is updated

146328 - SuSE SLES 11 SP4 SUSE-SU-2018:0362-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3145

Update Details
Risk is updated

146346 - SuSE Linux 42.3 openSUSE-SU-2018:0323-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3145

Update Details

Risk is updated

146405 - SuSE SLES 11 SP4 SUSE-SU-2018:0444-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3144

Update Details
Risk is updated

146427 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0532-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3144

Update Details
Risk is updated

146435 - SuSE Linux 42.3 openSUSE-SU-2018:0537-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3144

Update Details
Risk is updated

146515 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0812-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

146518 - SuSE SLES 11 SP4 SUSE-SU-2018:0810-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

146545 - SuSE Linux 42.3 openSUSE-SU-2018:0827-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium

CVE: CVE-2018-5732, CVE-2018-5733

Update Details

Risk is updated

147600 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0243-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-20406, CVE-2019-5010

Update Details

Risk is updated

160240 - CentOS 6 CESA-2017-1105 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3136, CVE-2017-3137

Update Details

Risk is updated

160243 - CentOS 7 CESA-2017-1095 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3136, CVE-2017-3137

Update Details

Risk is updated

160347 - CentOS 6 CESA-2018-0101 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3145

Update Details

Risk is updated

160350 - CentOS 7 CESA-2018-0102 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3145

Update Details

Risk is updated

160366 - CentOS 6 CESA-2018-0469 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

160378 - CentOS 7 CESA-2018-0483 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

163336 - Oracle Enterprise Linux ELSA-2017-1105 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137

Update Details
Risk is updated

163341 - Oracle Enterprise Linux ELSA-2017-1095 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137

Update Details
Risk is updated

163529 - Oracle Enterprise Linux ELSA-2018-0102 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3145

Update Details
Risk is updated

163530 - Oracle Enterprise Linux ELSA-2018-0101 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3145

Update Details

Risk is updated

163556 - Oracle Enterprise Linux ELSA-2018-0469 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

163558 - Oracle Enterprise Linux ELSA-2018-0483 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

170803 - Amazon Linux AMI ALAS-2017-826 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137

Update Details
Risk is updated

170931 - Amazon Linux AMI ALAS-2018-954 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3145

Update Details
Risk is updated

170951 - Amazon Linux AMI ALAS-2018-984 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

175159 - Scientific Linux Security ERRATA Important: bind on SL7.x x86_64 (1704-16936)

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

CVE: CVE-2017-3136, CVE-2017-3137

Update Details

Risk is updated

175163 - Scientific Linux Security ERRATA Important: bind on SL6.x i386/x86_64 (1704-17615)

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

Risk Level: Medium

CVE: CVE-2017-3136, CVE-2017-3137

Update Details

Risk is updated

175312 - Scientific Linux Security ERRATA Important: bind on SL6.x i386/x86_64 (1801-7533)

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

Risk Level: Medium

CVE: CVE-2017-3145

Update Details

Risk is updated

175313 - Scientific Linux Security ERRATA Important: bind on SL7.x x86_64 (1801-7212)

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

Risk Level: Medium

CVE: CVE-2017-3145

Update Details

Risk is updated

175329 - Scientific Linux Security ERRATA Important: dhcp on SL6.x i386/x86_64 (1803-1439)

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

Risk Level: Medium

CVE: CVE-2018-5732, CVE-2018-5733

Update Details

Risk is updated

175334 - Scientific Linux Security ERRATA Important: dhcp on SL7.x x86_64 (1803-1793)

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

Risk Level: Medium

CVE: CVE-2018-5732, CVE-2018-5733

Update Details

Risk is updated

182326 - FreeBSD BIND Multiple Vulnerabilities (c6861494-1ffb-11e7-934d-d05099c0ae8c)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Update Details
Risk is updated

182633 - FreeBSD isc-dhcp Multiple Vulnerabilities (2040c7f5-1e3a-11e8-8ae9-0050569f0b83)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5732, CVE-2018-5733

Update Details
Risk is updated

185672 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10, 17.04 USN-3259-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Update Details
Risk is updated

186065 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3535-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3145

Update Details
Risk is updated

191987 - Fedora Linux 25 FEDORA-2017-44e494db1e Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Update Details
Risk is updated

191989 - Fedora Linux 25 FEDORA-2017-ee4b0f53cb Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Update Details

Risk is updated

191992 - Fedora Linux 26 FEDORA-2017-f9f909a7b7 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Update Details
Risk is updated

192001 - Fedora Linux 26 FEDORA-2017-a354efc764 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Update Details
Risk is updated

192012 - Fedora Linux 24 FEDORA-2017-0a876b0ba5 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Update Details
Risk is updated

192075 - Fedora Linux 24 FEDORA-2017-edce28f24b Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3136, CVE-2017-3137, CVE-2017-3138

Update Details
Risk is updated

193203 - Fedora Linux 27 FEDORA-2018-97bdb9ba32 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3145

Update Details
Risk is updated

193219 - Fedora Linux 26 FEDORA-2018-6550550774 Update Is Not Installed

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

CVE: CVE-2017-3145

Update Details

Risk is updated

193364 - Fedora Linux 27 FEDORA-2018-5051dbd15e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5732, CVE-2018-5733

Update Details

Risk is updated

193982 - Fedora Linux 27 FEDORA-2018-c0f12f789e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3145, CVE-2018-5738

Update Details

Risk is updated

194098 - Fedora Linux 27 FEDORA-2018-90f8fbd58e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3145, CVE-2018-5738, CVE-2018-5740

Update Details

Risk is updated

194316 - Fedora Linux 27 FEDORA-2018-54d84b0b0c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3145, CVE-2018-5738, CVE-2018-5741

Update Details

Risk is updated

194582 - Fedora Linux 29 FEDORA-2018-b38a4dd0c7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19789, CVE-2018-19790

Update Details

Risk is updated

194586 - Fedora Linux 29 FEDORA-2018-8d3a9bdff1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-19789, CVE-2018-19790

Update Details
Risk is updated

194600 - Fedora Linux 29 FEDORA-2018-84a1f77d89 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-19789, CVE-2018-19790

Update Details
Risk is updated

22329 - IBM AIX Bind Multiple Vulnerabilities (bind_advisory16.asc)

Category: SSH Module -> NonIntrusive -> AIX Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

23308 - (HPESBUX03772) HP-UX BIND Named Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> HP-UX Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3140, CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

23414 - (HPESBUX03747) HP-UX BIND Remote Denial of Service Vulnerabilities

Category: SSH Module -> NonIntrusive -> HP-UX Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3135, CVE-2017-3136

Update Details
Risk is updated

88841 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-011-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-9778

Update Details

Risk is updated

88847 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-041-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3135

Update Details
Risk is updated

88870 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-165-01 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3140

Update Details
Risk is updated

88875 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2017-180-02 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

130709 - Debian Linux 8.0 DSA-3795-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3135

Update Details
Risk is updated

130813 - Debian Linux 8.0 DSA-3904-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

131275 - Debian Linux 9.0 DSA-4367-1 Update Is Not Installed

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

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

Update Details

Risk is updated

132386 - Oracle VM OVMSA-2017-0122 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3142, CVE-2017-3143

Update Details

Risk is updated

141425 - Red Hat Enterprise Linux RHSA-2017-0276 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3135

Update Details

Risk is updated

141624 - Red Hat Enterprise Linux RHSA-2017-1680 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3142, CVE-2017-3143

Update Details

Risk is updated

141626 - Red Hat Enterprise Linux RHSA-2017-1679 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3142, CVE-2017-3143

Update Details

Risk is updated

145248 - SuSE SLES 11 SP4 SUSE-SU-2017:0595-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3135

Update Details

Risk is updated

145249 - SuSE SLES 12 SP1, 12 SP2, SLED 12 SP1, 12 SP2 SUSE-SU-2017:0596-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3135

Update Details
Risk is updated

145418 - SuSE SLES 11 SP4 SUSE-SU-2017:1737-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

145430 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:1736-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

145526 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0620-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3135

Update Details
Risk is updated

145575 - SuSE Linux 42.2 openSUSE-SU-2017:1809-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

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

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-16864, CVE-2018-16865, CVE-2018-16866

Update Details

Risk is updated

147572 - SuSE Linux 42.3 openSUSE-SU-2019:0097-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-16864, CVE-2018-16865, CVE-2018-16866

Update Details
Risk is updated

160211 - CentOS 7 CESA-2017-0276 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3135

Update Details
Risk is updated

160279 - CentOS 7 CESA-2017-1680 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

160281 - CentOS 6 CESA-2017-1679 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

163281 - Oracle Enterprise Linux ELSA-2017-0276 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3135

Update Details
Risk is updated

163387 - Oracle Enterprise Linux ELSA-2017-1679 Update Is Not Installed

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

CVE: CVE-2017-3142, CVE-2017-3143

Update Details

Risk is updated

163389 - Oracle Enterprise Linux ELSA-2017-1680 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3142, CVE-2017-3143

Update Details

Risk is updated

170835 - Amazon Linux AMI ALAS-2017-858 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-3142, CVE-2017-3143

Update Details

Risk is updated

175115 - Scientific Linux Security ERRATA Moderate: bind on SL7.x x86_64 (1702-3607)

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

Risk Level: Medium

CVE: CVE-2017-3135

Update Details

Risk is updated

175199 - Scientific Linux Security ERRATA Important: bind on SL7.x x86_64 (1707-401)

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

Risk Level: Medium

CVE: CVE-2017-3142, CVE-2017-3143

Update Details

Risk is updated

175202 - Scientific Linux Security ERRATA Important: bind on SL6.x i386/x86_64 (1707-749)

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

Risk Level: Medium

CVE: CVE-2017-3142, CVE-2017-3143

Update Details

Risk is updated

185590 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3201-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3135

Update Details
Risk is updated

185766 - Ubuntu Linux 14.04, 16.04, 16.10, 17.04 USN-3346-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

185872 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3346-2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

191705 - Fedora Linux 25 FEDORA-2017-2b46c8b6c2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3135

Update Details
Risk is updated

191741 - Fedora Linux 24 FEDORA-2017-27099c270a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3135

Update Details
Risk is updated

192278 - Fedora Linux 26 FEDORA-2017-43613b15ff Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3140

Update Details

Risk is updated

192315 - Fedora Linux 26 FEDORA-2017-30f678e62a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

192336 - Fedora Linux 25 FEDORA-2017-167cfa7b09 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3140, CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

192343 - Fedora Linux 25 FEDORA-2017-d04f7ddd73 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3140, CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

192353 - Fedora Linux 26 FEDORA-2017-87f1f8c798 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3140, CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

192375 - Fedora Linux 24 FEDORA-2017-001f135337 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-3140, CVE-2017-3142, CVE-2017-3143

Update Details
Risk is updated

192450 - Fedora Linux 24 FEDORA-2017-59127a606c Update Is Not Installed

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

CVE: CVE-2017-3142, CVE-2017-3143

Update Details

Risk is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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