2019-JAN-09
FSL version 7.6.89

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

163782 - Oracle Enterprise Linux ELSA-2019-4316 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9728, CVE-2015-7837, CVE-2016-3713, CVE-2016-3841, CVE-2017-13168, CVE-2017-14051, CVE-2017-17450, CVE-2017-17805, CVE-2017-17806, CVE-2017-18017, CVE-2017-18079, CVE-2018-1000004, CVE-2018-1000204, CVE-2018-10021, CVE-2018-10902, CVE-2018-1092, CVE-2018-18710, CVE-2018-5848, CVE-2018-7755, CVE-2018-7757, CVE-2018-7995, CVE-2018-9516

Description

The scan detected that the host is missing the following update:
ELSA-2019-4316

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-January/008358.html
http://oss.oracle.com/pipermail/el-errata/2019-January/008357.html

OEL7
x86_64
kernel-uek-debug-3.8.13-118.29.1.el7uek
dtrace-modules-3.8.13-118.29.1.el7uek-0.4.5-3.el7
kernel-uek-doc-3.8.13-118.29.1.el7uek
kernel-uek-devel-3.8.13-118.29.1.el7uek
kernel-uek-firmware-3.8.13-118.29.1.el7uek
kernel-uek-3.8.13-118.29.1.el7uek
kernel-uek-debug-devel-3.8.13-118.29.1.el7uek

OEL6
x86_64
kernel-uek-3.8.13-118.29.1.el6uek
kernel-uek-devel-3.8.13-118.29.1.el6uek
kernel-uek-debug-3.8.13-118.29.1.el6uek
kernel-uek-firmware-3.8.13-118.29.1.el6uek
dtrace-modules-3.8.13-118.29.1.el6uek-0.4.5-3.el6
kernel-uek-debug-devel-3.8.13-118.29.1.el6uek
kernel-uek-doc-3.8.13-118.29.1.el6uek

24608 - (MSPT-Jan2019) Microsoft Windows DHCP Client Remote Code Execution (CVE-2019-0547)

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

Risk Level: High

CVE: CVE-2019-0547

Description

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

Observation

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

The flaw lies in the DHCP client. Successful exploitation by a remote attacker could result in arbitrary code execution.

163783 - Oracle Enterprise Linux ELSA-2019-4315 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-18079, CVE-2017-18174, CVE-2017-18221, CVE-2017-18255, CVE-2017-9725, CVE-2018-1092, CVE-2018-7995, CVE-2018-9363, CVE-2018-9516

Description

The scan detected that the host is missing the following update:
ELSA-2019-4315

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-January/008354.html
http://oss.oracle.com/pipermail/el-errata/2019-January/008355.html

OEL7
x86_64
kernel-uek-doc-4.1.12-124.24.1.el7uek
kernel-uek-debug-4.1.12-124.24.1.el7uek
kernel-uek-firmware-4.1.12-124.24.1.el7uek
kernel-uek-devel-4.1.12-124.24.1.el7uek
kernel-uek-4.1.12-124.24.1.el7uek
kernel-uek-debug-devel-4.1.12-124.24.1.el7uek

OEL6
x86_64
kernel-uek-devel-4.1.12-124.24.1.el6uek
kernel-uek-4.1.12-124.24.1.el6uek
kernel-uek-debug-devel-4.1.12-124.24.1.el6uek
kernel-uek-firmware-4.1.12-124.24.1.el6uek
kernel-uek-doc-4.1.12-124.24.1.el6uek
kernel-uek-debug-4.1.12-124.24.1.el6uek

24575 - (MSPT-Jan2019) Microsoft ASP.NET Core Denial of Service (CVE-2019-0564)

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

Risk Level: High

CVE: CVE-2019-0564

Description

A vulnerability in some versions of Microsoft ASP.NET Core could lead to a denial of service.

Observation

A vulnerability in some versions of Microsoft ASP.NET Core could lead to a denial of service.

The flaw is due to improper handling of Web Requests. Successful exploitation by a remote attacker could result in a denial of service condition.

24576 - (MSPT-Jan2019) Microsoft ASP.NET Core Denial of Service (CVE-2019-0548)

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

Risk Level: High

CVE: CVE-2019-0548

Description

A vulnerability in some versions of Microsoft ASP.NET Core could lead to a denial of service.

Observation

A vulnerability in some versions of Microsoft ASP.NET Core could lead to a denial of service.

The flaw is due to improper handling of web requests. Successful exploitation by a remote attacker could result in a denial of service condition.

24579 - (MSPT-Jan2019) Microsoft Jet Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0575)

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

Risk Level: High

CVE: CVE-2019-0575

Description

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

Observation

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

The flaw lies in the 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.

24580 - (MSPT-Jan2019) Microsoft Jet Improperly Handles Objects In Memory Remote Code Execution (CVE-2019-0576)

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

Risk Level: High

CVE: CVE-2019-0576

Description

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

Observation

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

The flaw lies in 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.

24581 - (MSPT-Jan2019) Microsoft Jet Improperly Handles Objects In Memory Remote Code Execution (CVE-2019-0577)

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

Risk Level: High

CVE: CVE-2019-0577

Description

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

Observation

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

The flaw lies in 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.

24582 - (MSPT-Jan2019) Microsoft Jet Improperly Handles Objects In Memory Remote Code Execution (CVE-2019-0579)

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

Risk Level: High

CVE: CVE-2019-0579

Description

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

Observation

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

The flaw lies in 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.

24583 - (MSPT-Jan2019) Microsoft Jet Improperly Handles Objects In Memory Remote Code Execution (CVE-2019-0580)

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

Risk Level: High

CVE: CVE-2019-0580

Description

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

Observation

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

The flaw lies in 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.

24584 - (MSPT-Jan2019) Microsoft Jet Improperly Handles Objects In Memory Remote Code Execution (CVE-2019-0581)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2019-0581

Description

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

Observation

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

The flaw lies in 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.

24585 - (MSPT-Jan2019) Microsoft Jet Improperly Handles Objects In Memory Remote Code Execution (CVE-2019-0582)

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

Risk Level: High

CVE: CVE-2019-0582

Description

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

Observation

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

The flaw lies in 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.

24587 - (MSPT-Jan2019) Microsoft Jet Improperly Handles Objects In Memory Remote Code Execution (CVE-2019-0583)

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

Risk Level: High

CVE: CVE-2019-0583

Description

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

Observation

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

The flaw lies in 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.

24588 - (MSPT-Jan2019) Microsoft Jet Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0584)

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

Risk Level: High

CVE: CVE-2019-0584

Description

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

Observation

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

The flaw lies in 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.

24592 - (MSPT-Jan2019) Microsoft Edge Chakra Remote Code Execution (CVE-2019-0568)

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

Risk Level: High

CVE: CVE-2019-0568

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 Chakra 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.

24593 - (MSPT-Jan2019) Microsoft Edge Chakra Remote Code Execution (CVE-2019-0567)

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

Risk Level: High

CVE: CVE-2019-0567

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 Chakra 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.

24594 - (MSPT-Jan2019) Microsoft Chakra Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0539)

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

Risk Level: High

CVE: CVE-2019-0539

Description

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

Observation

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

The flaw lies in the Improperly Handles Objects in Memory 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.

24596 - (MSPT-Jan2019) Microsoft Edge Improperly Accesses Objects in Memory Remote Code Execution (CVE-2019-0565)

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

Risk Level: High

CVE: CVE-2019-0565

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 Accesses Objects in Memory 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.

24597 - (MSPT-Jan2019) Microsoft Jet Improperly Handles Objects in Memory Remote Code Execution (CVE-2019-0578)

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

Risk Level: High

CVE: CVE-2019-0578

Description

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

Observation

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

The flaw lies in the Improperly Handles Objects in Memory 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.

24598 - (MSPT-Jan2019) Microsoft Windows Jet Database Engine Remote Code Execution (CVE-2019-0538)

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

Risk Level: High

CVE: CVE-2019-0538

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.

24610 - (MSPT-Jan2019) Microsoft Internet Explorer Remote Code Execution (CVE-2019-0541)

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

Risk Level: High

CVE: CVE-2019-0541

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 is due to improper handling of input. 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.

24612 - (MSPT-Jan2019) Microsoft Windows Hyper-V Remote Code Execution (CVE-2019-0550)

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

Risk Level: High

CVE: CVE-2019-0550

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 Hyper-V 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.

24613 - (MSPT-Jan2019) Microsoft Windows Hyper-V Remote Code Execution (CVE-2019-0551)

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

Risk Level: High

CVE: CVE-2019-0551

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 Hyper-V 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.

24619 - (MSPT-Jan2019) Microsoft Windows Visual Studio Remote Code Execution (CVE-2019-0546)

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

Risk Level: High

CVE: CVE-2019-0546

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 Visual Studio 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.

24623 - (MSPT-Jan2019) Microsoft Word Improperly Handle Objects in Memory Remote Code Execution (CVE-2019-0585)

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

Risk Level: High

CVE: CVE-2019-0585

Description

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

Observation

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

The flaw lies in the Improperly Handle Objects in Memory 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.

24625 - (MSPT-Jan2019) Microsoft Exchange Improperly Handle Objects in Memory Remote Code Execution (CVE-2019-0586)

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

Risk Level: High

CVE: CVE-2019-0586

Description

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

Observation

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

The flaw lies in the Improperly Handle Objects in Memory 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.

147518 - SuSE SLES 12 SP4, SLED 12 SP4 SUSE-SU-2019:0003-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-17963, CVE-2018-18849, CVE-2018-18883, CVE-2018-19665, CVE-2018-19961, CVE-2018-19962, CVE-2018-19963, CVE-2018-19964, CVE-2018-19965, CVE-2018-19966, CVE-2018-19967

Description

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

SUSE-SU-2019:0003-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005011.html

SuSE SLED 12 SP4
x86_64
xen-libs-32bit-4.11.1_02-2.3.1
xen-libs-debuginfo-4.11.1_02-2.3.1
xen-debugsource-4.11.1_02-2.3.1
xen-libs-4.11.1_02-2.3.1
xen-libs-debuginfo-32bit-4.11.1_02-2.3.1
xen-4.11.1_02-2.3.1

SuSE SLES 12 SP4
x86_64
xen-libs-32bit-4.11.1_02-2.3.1
xen-libs-debuginfo-4.11.1_02-2.3.1
xen-tools-domU-4.11.1_02-2.3.1
xen-tools-domU-debuginfo-4.11.1_02-2.3.1
xen-debugsource-4.11.1_02-2.3.1
xen-doc-html-4.11.1_02-2.3.1
xen-tools-4.11.1_02-2.3.1
xen-libs-4.11.1_02-2.3.1
xen-libs-debuginfo-32bit-4.11.1_02-2.3.1
xen-4.11.1_02-2.3.1
xen-tools-debuginfo-4.11.1_02-2.3.1

147520 - SuSE SLES 12 SP3, 12 SP4, SLED 12 SP3, 12 SP4 SUSE-SU-2019:0019-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19788

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0019-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005017.html

SuSE SLES 12 SP3
x86_64
polkit-debugsource-0.113-5.15.1
polkit-debuginfo-0.113-5.15.1
polkit-0.113-5.15.1
libpolkit0-debuginfo-0.113-5.15.1
typelib-1_0-Polkit-1_0-0.113-5.15.1
libpolkit0-0.113-5.15.1

SuSE SLES 12 SP4

x86_64
polkit-debugsource-0.113-5.15.1
polkit-debuginfo-0.113-5.15.1
polkit-0.113-5.15.1
libpolkit0-debuginfo-0.113-5.15.1
typelib-1_0-Polkit-1_0-0.113-5.15.1
libpolkit0-0.113-5.15.1

SuSE SLED 12 SP4
x86_64
polkit-debugsource-0.113-5.15.1
libpolkit0-debuginfo-32bit-0.113-5.15.1
polkit-debuginfo-0.113-5.15.1
polkit-0.113-5.15.1
libpolkit0-32bit-0.113-5.15.1
typelib-1_0-Polkit-1_0-0.113-5.15.1
libpolkit0-debuginfo-0.113-5.15.1
libpolkit0-0.113-5.15.1

SuSE SLED 12 SP3
x86_64
polkit-debugsource-0.113-5.15.1
libpolkit0-debuginfo-32bit-0.113-5.15.1
polkit-debuginfo-0.113-5.15.1
polkit-0.113-5.15.1
libpolkit0-32bit-0.113-5.15.1
typelib-1_0-Polkit-1_0-0.113-5.15.1
libpolkit0-debuginfo-0.113-5.15.1
libpolkit0-0.113-5.15.1

147521 - SuSE SLES 11 SP4 SUSE-SU-2019:13921-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13672, CVE-2018-10839, CVE-2018-17958, CVE-2018-17962, CVE-2018-17963, CVE-2018-18438, CVE-2018-18849, CVE-2018-19665, CVE-2018-19961, CVE-2018-19962, CVE-2018-19965, CVE-2018-19966, CVE-2018-19967

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13921-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005012.html

SuSE SLES 11 SP4
x86_64
xen-libs-32bit-4.4.4_38-61.40.1
xen-4.4.4_38-61.40.1
xen-libs-4.4.4_38-61.40.1
xen-kmp-default-4.4.4_38_3.0.101_108.84-61.40.1
xen-tools-domU-4.4.4_38-61.40.1
xen-doc-html-4.4.4_38-61.40.1
xen-tools-4.4.4_38-61.40.1

i586

xen-tools-domU-4.4.4_38-61.40.1
xen-kmp-default-4.4.4_38_3.0.101_108.84-61.40.1
xen-kmp-pae-4.4.4_38_3.0.101_108.84-61.40.1
xen-libs-4.4.4_38-61.40.1

147522 - SuSE SLES 11 SP4 SUSE-SU-2019:13924-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-2775, CVE-2016-6893, CVE-2018-0618, CVE-2018-13796, CVE-2018-5950

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:13924-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005015.html

SuSE SLES 11 SP4
i586
mailman-2.1.15-9.6.6.1

x86_64
mailman-2.1.15-9.6.6.1

147523 - SuSE SLED 15 SUSE-SU-2019:0005-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5804, CVE-2018-5813, CVE-2018-5815, CVE-2018-5816

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0005-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005010.html

SuSE SLED 15
x86_64
libraw-devel-0.18.9-3.5.1
libraw16-0.18.9-3.5.1
libraw-debugsource-0.18.9-3.5.1
libraw-debuginfo-0.18.9-3.5.1
libraw16-debuginfo-0.18.9-3.5.1

160502 - CentOS 7 CESA-2019-0022 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19115

Description

The scan detected that the host is missing the following update:
CESA-2019-0022

Observation

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

http://lists.centos.org/pipermail/centos-announce/2019-January/023140.html

CentOS 7
x86_64
keepalived-1.3.5-8.el7_6

163781 - Oracle Enterprise Linux ELSA-2019-0022 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19115

Description

The scan detected that the host is missing the following update:
ELSA-2019-0022

Observation

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

http://oss.oracle.com/pipermail/el-errata/2019-January/008359.html

OEL7
x86_64
keepalived-1.3.5-8.el7_6

175516 - Scientific Linux Security ERRATA Important: keepalived on SL7.x x86_64 (1901-78)

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

Risk Level: High

CVE: CVE-2018-19115

Description

The scan detected that the host is missing the following update:
Security ERRATA Important: keepalived on SL7.x x86_64 (1901-78)

Observation

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

https://listserv.fnal.gov/scripts/wa.exe?A2=ind1901&L=scientific-linux-errata&F=&S=&P=78

SL7

x86_64
keepalived-debuginfo-1.3.5-8.el7_6
keepalived-1.3.5-8.el7_6

194645 - Fedora Linux 28 FEDORA-2018-166b220ff1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-13112, CVE-2018-17580, CVE-2018-17582, CVE-2018-17974, CVE-2018-18407, CVE-2018-18408

Description

The scan detected that the host is missing the following update:
FEDORA-2018-166b220ff1

Observation

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

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

Fedora Core 28

tcpreplay-4.3.1-1.fc28

194649 - Fedora Linux 29 FEDORA-2018-5f91054677 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-13112, CVE-2018-17580, CVE-2018-17582, CVE-2018-17974, CVE-2018-18407, CVE-2018-18408

Description

The scan detected that the host is missing the following update:
FEDORA-2018-5f91054677

Observation

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

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

Fedora Core 29

tcpreplay-4.3.1-1.fc29

196227 - Red Hat Enterprise Linux RHSA-2019-0001 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18311, CVE-2018-18312, CVE-2018-18313, CVE-2018-18314

Description

The scan detected that the host is missing the following update:
RHSA-2019-0001

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-January/msg00000.html

RHEL7S
noarch
rh-perl526-perl-ExtUtils-Miniperl-1.06-405.el7
rh-perl526-perl-Module-CoreList-tools-5.20181130-1.el7

RHEL7WS
x86_64
rh-perl526-perl-debuginfo-5.26.3-405.el7

noarch
rh-perl526-perl-ExtUtils-Miniperl-1.06-405.el7
rh-perl526-perl-Module-CoreList-tools-5.20181130-1.el7

196229 - Red Hat Enterprise Linux RHSA-2019-0010 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-18311, CVE-2018-18312, CVE-2018-18313, CVE-2018-18314

Description

The scan detected that the host is missing the following update:
RHSA-2019-0010

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-January/msg00001.html

RHEL6S
x86_64
rh-perl524-perl-tests-5.24.0-381.el6

noarch
rh-perl524-perl-Locale-Maketext-Simple-0.21-381.el6

RHEL6WS
x86_64
rh-perl524-perl-tests-5.24.0-381.el6

noarch
rh-perl524-perl-Locale-Maketext-Simple-0.21-381.el6

RHEL7S
x86_64
rh-perl524-perl-tests-5.24.0-381.el7

noarch
rh-perl524-perl-Locale-Maketext-Simple-0.21-381.el7

RHEL7WS
x86_64

rh-perl524-perl-tests-5.24.0-381.el7

noarch
rh-perl524-perl-Locale-Maketext-Simple-0.21-381.el7

196230 - Red Hat Enterprise Linux RHSA-2019-0022 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-19115

Description

The scan detected that the host is missing the following update:
RHSA-2019-0022

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-January/msg00003.html

RHEL7S
x86_64
keepalived-debuginfo-1.3.5-8.el7_6
keepalived-1.3.5-8.el7_6

RHEL7WS
x86_64
keepalived-debuginfo-1.3.5-8.el7_6
keepalived-1.3.5-8.el7_6

24577 - (MSPT-Jan2019) Microsoft .NET Framework Information Disclosure (CVE-2019-0545)

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

Risk Level: Medium

CVE: CVE-2019-0545

Description

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

Observation

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

The flaw lies in Cross-origin Resource Sharing (CORS) configurations. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

24605 - (MSPT-Jan2019) Microsoft XmlDocument AppContainer sandbox Privilege Escalation (CVE-2019-0555)

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

Risk Level: Medium

CVE: CVE-2019-0555

Description

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

Observation

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

The flaw lies in the AppContainer sandbox. Successful exploitation could allow a local user to gain elevated privileges.

24606 - (MSPT-Jan2019) Microsoft Windows COM Desktop Broker Privilege Escalation (CVE-2019-0552)

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

Risk Level: Medium

CVE: CVE-2019-0552

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 COM Desktop Broker 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.

24616 - (MSPT-Jan2019) Microsoft Office SharePoint Cross-site Scripting (CVE-2019-0556)

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

Risk Level: Medium

CVE: CVE-2019-0556

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 is due to improper handing of crafted web requests. 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.

24617 - (MSPT-Jan2019) Microsoft Office SharePoint Cross-site Scripting (CVE-2019-0557)

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

Risk Level: Medium

CVE: CVE-2019-0557

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 is due to improper handing of web requests. 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.

24618 - (MSPT-Jan2019) Microsoft Office SharePoint Cross-site Scripting (CVE-2019-0558)

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

Risk Level: Medium

CVE: CVE-2019-0558

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 is due to improper handing of web requests. 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.

147519 - SuSE SLED 12 SP3, 12 SP4 SUSE-SU-2019:0002-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5805, CVE-2018-5806, CVE-2018-5808

Description

The scan detected that the host is missing the following update:
SUSE-SU-2019:0002-1

Observation

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

http://lists.suse.com/pipermail/sle-security-updates/2019-January/005009.html

SuSE SLED 12 SP4
x86_64
libraw9-debuginfo-0.15.4-27.1
libraw-debugsource-0.15.4-27.1
libraw9-0.15.4-27.1

SuSE SLED 12 SP3
x86_64
libraw9-debuginfo-0.15.4-27.1
libraw-debugsource-0.15.4-27.1
libraw9-0.15.4-27.1

182879 - FreeBSD chromium Multiple Vulnerabilities (546d4dd4-10ea-11e9-b407-080027ef1a23)

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
chromium -- multiple vulnerabilities (546d4dd4-10ea-11e9-b407-080027ef1a23)

Observation

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

http://www.vuxml.org/freebsd/546d4dd4-10ea-11e9-b407-080027ef1a23.html

Affected packages:
chromium < 71.0.3578.80

182881 - FreeBSD chromium Use After Free In PDFium (720590df-10eb-11e9-b407-080027ef1a23)

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

Risk Level: Medium

CVE: CVE-2018-17481

Description

The scan detected that the host is missing the following update:
chromium -- Use after free in PDFium (720590df-10eb-11e9-b407-080027ef1a23)

Observation

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

http://www.vuxml.org/freebsd/720590df-10eb-11e9-b407-080027ef1a23.html

Affected packages:
chromium < 71.0.3578.98

194644 - Fedora Linux 29 FEDORA-2019-859384e002 Update Is Not Installed

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

Risk Level: Medium

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

Description

The scan detected that the host is missing the following update:
FEDORA-2019-859384e002

Observation

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

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

Fedora Core 29

chromium-71.0.3578.98-1.fc29

196228 - Red Hat Enterprise Linux RHSA-2019-0036 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1102

Description

The scan detected that the host is missing the following update:
RHSA-2019-0036

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-January/msg00005.html

RHEL7S
x86_64
source-to-image-1.1.13-1.el7

24586 - (MSPT-Jan2019) Microsoft Windows Kernel Information Disclosure (CVE-2019-0536)

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

Risk Level: Medium

CVE: CVE-2019-0536

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.

24589 - (MSPT-Jan2019) Microsoft Windows Kernel Information Disclosure (CVE-2019-0569)

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

Risk Level: Medium

CVE: CVE-2019-0569

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.

24590 - (MSPT-Jan2019) Microsoft Windows Kernel Information Disclosure (CVE-2019-0549)

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

Risk Level: Medium

CVE: CVE-2019-0549

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.

24591 - (MSPT-Jan2019) Microsoft Windows Kernel Information Disclosure (CVE-2019-0554)

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

Risk Level: Medium

CVE: CVE-2019-0554

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.

24595 - (MSPT-Jan2019) Microsoft Edge Broker COM object Privilege Escalation (CVE-2019-0566)

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

Risk Level: Medium

CVE: CVE-2019-0566

Description

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

Observation

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

The flaw lies in the Broker COM object 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.

24599 - (MSPT-Jan2019) Microsoft Windows Data Sharing Privilege Escalation (CVE-2019-0574)

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

Risk Level: Medium

CVE: CVE-2019-0574

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 Data Sharing 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.

24600 - (MSPT-Jan2019) Microsoft Windows Improperly Handles Authentication Requests Privilege Escalation (CVE-2019-0543)

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

Risk Level: Medium

CVE: CVE-2019-0543

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 Improperly Handles Authentication Requests 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.

24601 - (MSPT-Jan2019) Microsoft Windows Data Sharing Privilege Escalation (CVE-2019-0573)

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

Risk Level: Medium

CVE: CVE-2019-0573

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 Data Sharing 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.

24602 - (MSPT-Jan2019) Microsoft Windows Data Sharing Privilege Escalation (CVE-2019-0572)

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

Risk Level: Medium

CVE: CVE-2019-0572

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 Data Sharing 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.

24603 - (MSPT-Jan2019) Microsoft Windows Data Sharing Privilege Escalation (CVE-2019-0571)

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

Risk Level: Medium

CVE: CVE-2019-0571

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 Data Sharing 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.

24604 - (MSPT-Jan2019) Microsoft Windows Runtime Privilege Escalation (CVE-2019-0570)

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

Risk Level: Medium

CVE: CVE-2019-0570

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 Runtime 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.

24614 - (MSPT-Jan2019) Microsoft Visual Studio Improperly Discloses File Contents Information Disclosure (CVE-2019-0537)

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

Risk Level: Medium

CVE: CVE-2019-0537

Description

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

Observation

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

The flaw lies in the Improperly Discloses File Contents 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.

24615 - (MSPT-Jan2019) Microsoft SharePoint Elevation of Privilege (CVE-2019-0562)

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

Risk Level: Medium

CVE: CVE-2019-0562

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 is due to improper handing of crafted web requests. Successful exploitation could allow an authenticated user to gain elevated privileges.

24620 - (MSPT-Jan2019) Microsoft Outlook Improperly Handles Messages Information Disclosure (CVE-2019-0559)

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

Risk Level: Medium

CVE: CVE-2019-0559

Description

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

Observation

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

The flaw lies in the Improperly Handles Messages 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.

24621 - (MSPT-Jan2019) Microsoft Office Improperly Discloses Contents of Its Memory Information Disclosure (CVE-2019-0560)

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

Risk Level: Medium

CVE: CVE-2019-0560

Description

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

Observation

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

The flaw lies in the Improperly Discloses Contents of Its Memory 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.

24622 - (MSPT-Jan2019) Microsoft Word Macro Buttons Information Disclosure (CVE-2019-0561)

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

Risk Level: Medium

CVE: CVE-2019-0561

Description

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

Observation

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

The flaw lies in the Macro Buttons 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.

24624 - (MSPT-Jan2019) Microsoft Exchange PowerShell API Information Disclosure (CVE-2019-0588)

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

Risk Level: Medium

CVE: CVE-2019-0588

Description

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

Observation

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

The flaw lies in the PowerShell API 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.

24609 - (MSPT-Jan2019) Microsoft Windows Subsystem for Linux Information Disclosure (CVE-2019-0553)

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

Risk Level: Medium

CVE: CVE-2019-0553

Description

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

Observation

A vulnerability in some versions of Microsoft Windows Subsystem for Linux 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 have valid credentials to the vulnerable system.

194647 - Fedora Linux 28 FEDORA-2018-67e98d4b7a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-19787

Description

The scan detected that the host is missing the following update:
FEDORA-2018-67e98d4b7a

Observation

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

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

Fedora Core 28

python-lxml-4.2.5-1.fc28

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

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
DSA-4362-1

Observation

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

http://www.debian.org/security/2019/dsa-4362

Debian 9.0
all
thunderbird_1:60.4.0-1~deb9u1

182878 - FreeBSD Gitlab Multiple Vulnerabilities (b2f4ab91-0e6b-11e9-8700-001b217b3468)

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

Risk Level: Low

CVE: CVE-2018-20488, CVE-2018-20489, CVE-2018-20490, CVE-2018-20491, CVE-2018-20492, CVE-2018-20493, CVE-2018-20494, CVE-2018-20495, CVE-2018-20496, CVE-2018-20497, CVE-2018-20498, CVE-2018-20499, CVE-2018-20500, CVE-2018-20501, CVE-2018-20507

Description

The scan detected that the host is missing the following update:
Gitlab -- Multiple vulnerabilities (b2f4ab91-0e6b-11e9-8700-001b217b3468)

Observation

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

http://www.vuxml.org/freebsd/b2f4ab91-0e6b-11e9-8700-001b217b3468.html

Affected packages:
11.6.0 <= gitlab-ce < 11.6.1
11.5.0 <= gitlab-ce < 11.5.6

8.0.0 <= gitlab-ce < 11.4.13

182880 - FreeBSD gitea Insufficient Privilege Check (63e36475-119f-11e9-aba7-080027fee39c)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
gitea -- insufficient privilege check (63e36475-119f-11e9-aba7-080027fee39c)

Observation

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

http://www.vuxml.org/freebsd/63e36475-119f-11e9-aba7-080027fee39c.html

Affected packages:
gitea < 1.6.3

182882 - FreeBSD uriparser Out-of-bounds Read (924bd4f8-11e7-11e9-9fe8-5404a68ad561)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
uriparser -- Out-of-bounds read (924bd4f8-11e7-11e9-9fe8-5404a68ad561)

Observation

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

http://www.vuxml.org/freebsd/924bd4f8-11e7-11e9-9fe8-5404a68ad561.html

Affected packages:
uriparser < 0.9.1

182883 - FreeBSD Django Content Spoofing Possibility In The Default 404 Page (3e41c1a6-10bc-11e9-bd85-fcaa147e860e)

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

Risk Level: Low

CVE: CVE-2019-3498

Description

The scan detected that the host is missing the following update:
Django -- Content spoofing possibility in the default 404 page (3e41c1a6-10bc-11e9-bd85-fcaa147e860e)

Observation

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

http://www.vuxml.org/freebsd/3e41c1a6-10bc-11e9-bd85-fcaa147e860e.html

Affected packages:
py27-django111 < 1.11.18
py35-django111 < 1.11.18
py36-django111 < 1.11.18
py37-django111 < 1.11.18
py35-django20 < 2.0.10
py36-django20 < 2.0.10
py37-django20 < 2.0.10
py35-django21 < 2.1.5
py36-django21 < 2.1.5
py37-django21 < 2.1.5

194643 - Fedora Linux 29 FEDORA-2019-03b6506fd0 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-2019-03b6506fd0

Observation

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

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

Fedora Core 29

thunderbird-60.4.0-1.fc29

194646 - Fedora Linux 29 FEDORA-2019-d2cb69f11e Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20217

Description

The scan detected that the host is missing the following update:
FEDORA-2019-d2cb69f11e

Observation

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

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

Fedora Core 29

krb5-1.16.1-24.fc29

194648 - Fedora Linux 29 FEDORA-2019-f9d5bbef82 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-f9d5bbef82

Observation

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

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

Fedora Core 29

python3-docs-3.7.2-1.fc29
python3-3.7.2-1.fc29

194650 - Fedora Linux 29 FEDORA-2019-088875c43a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-20483

Description

The scan detected that the host is missing the following update:
FEDORA-2019-088875c43a

Observation

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

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

Fedora Core 29

wget-1.20.1-1.fc29

196226 - Red Hat Enterprise Linux RHSA-2019-0031 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

The scan detected that the host is missing the following update:
RHSA-2019-0031

Observation

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

http://www.redhat.com/archives/rhsa-announce/2019-January/msg00004.html

RHEL6_6S
x86_64
redhat-release-server-6Server-6.6.0.5.el6_6.3

24626 - (APSB19-01) Vulnerability In Adobe Flash Player

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

Feature and performance bugs are 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.

Feature and performance bugs are present in some versions of Adobe Flash Player.

The update provided by Adobe bulletin APSB19-01 resolves the issues. The target system is missing this update.

24627 - (APSB19-01) Vulnerability In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Description

Feature and performance bugs are 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.

Feature and performance bugs are present in some versions of Adobe Flash Player.

The update provided by Adobe bulletin APSB19-01 resolves the issues. The target system is missing this update.

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.

88981 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-283-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-17456

Update Details

Risk is updated

131217 - Debian Linux 9.0 DSA-4311-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-17456

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

182818 - FreeBSD Libgit2 Multiple Vulnerabilities (8c08ab4c-d06c-11e8-b35c-001b217b3468)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-17456

Update Details
Risk is updated

186425 - Ubuntu Linux 14.04, 16.04, 18.04 USN-3791-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-17456

Update Details
Risk is updated

191340 - Fedora Linux 23 FEDORA-2016-2a159ef513 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-7035

Update Details
Risk is updated

191342 - Fedora Linux 24 FEDORA-2016-242ff9a2fa Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-7035

Update Details
Risk is updated

191354 - Fedora Linux 25 FEDORA-2016-c1cbcc4528 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-7035

Update Details
Risk is updated

194259 - Fedora Linux 29 FEDORA-2018-abfd4c6ac3 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-17456

Update Details
Risk is updated

194280 - Fedora Linux 29 FEDORA-2018-06090dff59 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-17456

Update Details
Risk is updated

194561 - Fedora Linux 29 FEDORA-2018-3fbc181b3e Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-19044, CVE-2018-19045, CVE-2018-19046, CVE-2018-19047, CVE-2018-19115

Update Details
Risk is updated

194617 - Fedora Linux 29 FEDORA-2018-de3a0ba76e Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-17825

Update Details
Risk is updated

194619 - Fedora Linux 28 FEDORA-2018-4b8a18767b Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2018-17825

Update Details

Risk is updated

132486 - Oracle VM OVMSA-2018-0270 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000805

Update Details

Risk is updated

160480 - CentOS 6 CESA-2018-3406 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000805

Update Details

Risk is updated

160488 - CentOS 7 CESA-2018-3347 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000805

Update Details

Risk is updated

163749 - Oracle Enterprise Linux ELSA-2018-3406 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000805

Update Details

Risk is updated

163756 - Oracle Enterprise Linux ELSA-2018-3347 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000805

Update Details

Risk is updated

171030 - Amazon Linux AMI ALAS-2018-1096 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-1000805

Update Details
Risk is updated

175467 - Scientific Linux Security ERRATA Critical: python-paramiko on SL6.x (noarch) (1810-13335)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-2018-1000805

Update Details
Risk is updated

175479 - Scientific Linux Security ERRATA Critical: python-paramiko on SL7.x (noarch) (1811-13751)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-2018-1000805

Update Details
Risk is updated

186434 - Ubuntu Linux 18.10 USN-3796-3 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-1000805

Update Details
Risk is updated

186446 - Ubuntu Linux 14.04, 16.04, 18.04 USN-3796-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-1000805

Update Details
Risk is updated

194338 - Fedora Linux 28 FEDORA-2018-3ff1cb628b Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-1000805

Update Details
Risk is updated

194365 - Fedora Linux 29 FEDORA-2018-ea6b328afd Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-1000805

Update Details
Risk is updated

194634 - Fedora Linux 29 FEDORA-2018-801432b551 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-20337, CVE-2018-20363, CVE-2018-20364, CVE-2018-20365

Update Details
Risk is updated

196137 - Red Hat Enterprise Linux RHSA-2018-3347 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-1000805

Update Details
Risk is updated

196177 - Red Hat Enterprise Linux RHSA-2018-3406 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-1000805

Update Details
Risk is updated

194521 - Fedora Linux 29 FEDORA-2018-f6b7df660d Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-19591

Update Details
Risk is updated

24305 - Apache Tomcat Vulnerability Prior To 9.0.12

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server
Risk Level: Medium
CVE: CVE-2018-11784

Update Details

Risk is updated

24349 - Apache Tomcat Vulnerability Prior To 8.5.34

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

Risk Level: Medium

CVE: CVE-2018-11784

Update Details

Risk is updated

24353 - Apache Tomcat Vulnerability Prior To 7.0.91

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

Risk Level: Medium

CVE: CVE-2018-11784

Update Details

Risk is updated

147256 - SuSE Linux 42.3 openSUSE-SU-2018:3453-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11784

Update Details

Risk is updated

147302 - SuSE SLES 12 SP3 SUSE-SU-2018:3393-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11784

Update Details

Risk is updated

147390 - SuSE SLES 11 SP4 SUSE-SU-2018:3935-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-11784

Update Details

Risk is updated

147424 - SuSE Linux 15.0 openSUSE-SU-2018:4042-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-11784

Update Details
Risk is updated

147506 - SuSE Linux 15.0 openSUSE-SU-2019:1-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-20184, CVE-2018-20189

Update Details
Risk is updated

147516 - SuSE Linux 42.3 openSUSE-SU-2018:4313-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-20184, CVE-2018-20189

Update Details
Risk is updated

171034 - Amazon Linux AMI ALAS-2018-1099 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-11784

Update Details
Risk is updated

182814 - FreeBSD Django Password Hash Disclosure (004d8c23-c710-11e8-98c7-000c29434208)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-16984

Update Details
Risk is updated

186430 - Ubuntu Linux 14.04, 16.04 USN-3787-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-11784

Update Details
Risk is updated

160496 - CentOS 7 CESA-2018-3663 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Low
CVE: CVE-2018-14650

Update Details
Risk is updated

163768 - Oracle Enterprise Linux ELSA-2018-3663 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Low
CVE: CVE-2018-14650

Update Details
Risk is updated

175499 - Scientific Linux Security ERRATA Moderate: sos-collector on SL7.x (noarch) (1811-14419)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: Low
CVE: CVE-2018-14650

Update Details
Risk is updated

194366 - Fedora Linux 29 FEDORA-2018-672c028631 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2018-14650

Update Details
Risk is updated

194388 - Fedora Linux 28 FEDORA-2018-1f3a47bfbb Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2018-14650

Update Details
Risk is updated

194390 - Fedora Linux 27 FEDORA-2018-f2f8571abd Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Low
CVE: CVE-2018-14650

Update Details

Risk is updated

196202 - Red Hat Enterprise Linux RHSA-2018-3663 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2018-14650

Update Details

Risk is updated

70014 - netbios-helpers.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com/

Multi-National Phone Support available here:

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

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