2018-JAN-09
FSL version 7.5.992

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

22923 - (MSPT-Jan2018) Microsoft Office Memory Handling Remote Code Execution (CVE-2018-0798)

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

Risk Level: High

CVE: CVE-2018-0798

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 a memory handling error. 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.

22945 - (MSPT-Jan2018) Microsoft Office Email Parsing Remote Code Execution (CVE-2018-0791)

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

Risk Level: High

CVE: CVE-2018-0791

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 Email Parsing 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.

22946 - (MSPT-Jan2018) Microsoft Office Memory Handling Remote Code Execution (CVE-2018-0792)

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

Risk Level: High

CVE: CVE-2018-0792

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 a memory handling error. 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.

22947 - (MSPT-Jan2018) Microsoft Office Memory Handling Remote Code Execution (CVE-2018-0794)

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

Risk Level: High

CVE: CVE-2018-0794

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 a memory handling error. 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.

22948 - (MSPT-Jan2018) Microsoft Office Memory Handling Remote Code Execution (CVE-2018-0796)

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

Risk Level: High

CVE: CVE-2018-0796

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 a memory handling error. 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.

22949 - (MSPT-Jan2018) Microsoft Office Memory Handling Remote Code Execution (CVE-2018-0801)

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

Risk Level: High

CVE: CVE-2018-0801

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 a memory handling error. 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.

22951 - (MSPT-Jan2018) Microsoft Office Memory Handling Remote Code Execution (CVE-2018-0795)

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

Risk Level: High

CVE: CVE-2018-0795

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 a memory handling error. 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.

22952 - (MSPT-Jan2018) Microsoft Office Email Parsing Remote Code Execution (CVE-2018-0793)

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

Risk Level: High

CVE: CVE-2018-0793

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 Email Parsing 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.

22953 - (MSPT-Jan2018) Microsoft Office RTF Handling Remote Code Execution (CVE-2018-0797)

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

Risk Level: High

CVE: CVE-2018-0797

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 RTF Handling 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.

22960 - (MSPT-Jan2018) Microsoft Office Memory Corurption Remote Code Execution (CVE-2018-0802)

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

Risk Level: High

CVE: CVE-2018-0802

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 Memory Corruption 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.

22964 - (MSPT-Jan2018) Microsoft Word Remote Code Execution Vulnerability (CVE-2018-0804)

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

Risk Level: High

CVE: CVE-2018-0804

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 a memory handling error. 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.

22965 - (MSPT-Jan2018) Microsoft Word Remote Code Execution Vulnerability (CVE-2018-0805)

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

Risk Level: High

CVE: CVE-2018-0805

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 a memory handling error. 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.

22966 - (MSPT-Jan2018) Microsoft Word Remote Code Execution Vulnerability (CVE-2018-0806)

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

Risk Level: High

CVE: CVE-2018-0806

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 a memory handling error. 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.

22967 - (MSPT-Jan2018) Microsoft Word Remote Code Execution Vulnerability (CVE-2018-0807)

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

Risk Level: High

CVE: CVE-2018-0807

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 a memory handling error. 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.

22968 - (MSPT-Jan2018) Microsoft Word Remote Code Execution Vulnerability (CVE-2018-0812)

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

Risk Level: High

CVE: CVE-2018-0812

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 a memory handling error. 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.

22969 - (APSB18-01) Vulnerability In Adobe Flash Player

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

Risk Level: Medium

CVE: CVE-2018-4871

Description

A 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.

A vulnerability is present in some versions of Adobe Flash Player. The flaw is due to an out-of-bounds read. Successful exploitation

could allow an attacker to disclose private information on the target system.

The update provided by Adobe bulletin APSB18-01 resolves the issue. The target system is missing this update.

22970 - (APSB18-01) Vulnerability In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2018-4871

Description

A 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.

A vulnerability is present in some versions of Adobe Flash Player. The flaw is due to an out-of-bounds read. Successful exploitation could allow an attacker to disclose private information on the target system.

The update provided by Adobe bulletin APSB18-01 resolves the issue. The target system is missing this update.

22900 - (MSPT-Jan2018) Microsoft Office Memory Handling Information Disclosure (CVE-2018-0790)

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

Risk Level: Medium

CVE: CVE-2018-0790

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 a memory handling error. 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.

22944 - (MSPT-Jan2018) Microsoft Office RFC2046 Information Disclosure (CVE-2018-0789)

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

Risk Level: Medium

CVE: CVE-2018-0789

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 RFC2046 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.

22950 - (MSPT-Jan2018) Microsoft Office Input Sanitization Security Bypass (CVE-2018-0799)

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

Risk Level: Medium

CVE: CVE-2018-0799

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 the Input Sanitization component. 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.

22954 - (MSPT-Jan2018) Microsoft .NET Framework Core Denial of Service (CVE-2018-0764)

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

Risk Level: Medium

CVE: CVE-2018-0764

Description

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

Observation

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

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

22961 - (MSPT-Jan2018) Microsoft .NET Framework Security Security Bypass (CVE-2018-0786)

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

Risk Level: Medium

CVE: CVE-2018-0786

Description

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

Observation

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

The flaw is due to improper handling of certificates. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions.

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.

193137 - Fedora Linux 26 FEDORA-2018-8ed5eff2c0 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17852, CVE-2017-17853, CVE-2017-17854, CVE-2017-17855, CVE-2017-17856, CVE-2017-17857, CVE-2017-17862, CVE-2017-17863, CVE-2017-17864

Update Details

Risk is updated

193141 - Fedora Linux 27 FEDORA-2018-22d5fa8a90 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-17852, CVE-2017-17853, CVE-2017-17854, CVE-2017-17855, CVE-2017-17856, CVE-2017-17857, CVE-2017-17862, CVE-2017-17863, CVE-2017-17864

Update Details

Risk is updated

141811 - Red Hat Enterprise Linux RHSA-2018-0011 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Update Details

Risk is updated

141812 - Red Hat Enterprise Linux RHSA-2018-0020 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Update Details

Risk is updated

141813 - Red Hat Enterprise Linux RHSA-2018-0027 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Update Details

Risk is updated

141814 - Red Hat Enterprise Linux RHSA-2018-0037 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Update Details

Risk is updated

141815 - Red Hat Enterprise Linux RHSA-2018-0007 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Update Details

Risk is updated

141816 - Red Hat Enterprise Linux RHSA-2018-0017 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Update Details

Risk is updated

141817 - Red Hat Enterprise Linux RHSA-2018-0008 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Update Details

Risk is updated

141818 - Red Hat Enterprise Linux RHSA-2018-0023 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Update Details

Risk is updated

141819 - Red Hat Enterprise Linux RHSA-2018-0012 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Update Details

Risk is updated

141820 - Red Hat Enterprise Linux RHSA-2018-0013 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

141821 - Red Hat Enterprise Linux RHSA-2018-0015 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

141822 - Red Hat Enterprise Linux RHSA-2018-0029 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

141823 - Red Hat Enterprise Linux RHSA-2018-0039 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

141824 - Red Hat Enterprise Linux RHSA-2018-0036 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

141825 - Red Hat Enterprise Linux RHSA-2018-0024 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

141826 - Red Hat Enterprise Linux RHSA-2018-0034 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

141827 - Red Hat Enterprise Linux RHSA-2018-0009 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Update Details
Risk is updated

141828 - Red Hat Enterprise Linux RHSA-2018-0014 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

141829 - Red Hat Enterprise Linux RHSA-2018-0030 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

141830 - Red Hat Enterprise Linux RHSA-2018-0040 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

141831 - Red Hat Enterprise Linux RHSA-2018-0038 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details

Risk is updated

141832 - Red Hat Enterprise Linux RHSA-2018-0031 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Update Details

Risk is updated

141833 - Red Hat Enterprise Linux RHSA-2018-0018 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Update Details

Risk is updated

141834 - Red Hat Enterprise Linux RHSA-2018-0022 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Update Details

Risk is updated

146196 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0008-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5715

Update Details

Risk is updated

146199 - SuSE SLES 11 SP4 SUSE-SU-2018:0019-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-2633, CVE-2017-5715

Update Details

Risk is updated

146200 - SuSE Linux 42.3 openSUSE-SU-2018:0013-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

146204 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0007-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

146206 - SuSE SLES 11 SP4 SUSE-SU-2018:0009-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

146207 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0006-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

163517 - Oracle Enterprise Linux ELSA-2018-0012 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

163518 - Oracle Enterprise Linux ELSA-2018-0007 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Update Details
Risk is updated

163519 - Oracle Enterprise Linux ELSA-2018-0013 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

170916 - Amazon Linux AMI ALAS-2018-939 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5754

Update Details
Risk is updated

175302 - Scientific Linux Security ERRATA Important: kernel on SL6.x i386/x86_64 (1801-769)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Update Details
Risk is updated

175303 - Scientific Linux Security ERRATA Important: libvirt on SL7.x x86_64 (1801-2808)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details
Risk is updated

175304 - Scientific Linux Security ERRATA Important: kernel on SL7.x x86_64 (1801-78)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

Update Details
Risk is updated

175305 - Scientific Linux Security ERRATA Important: qemu-kvm on SL7.x x86_64 (1801-2480)

Category: SSH Module -> NonIntrusive -> Scientific Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-2017-5715

Update Details

Risk is updated

175306 - Scientific Linux Security ERRATA Important: microcode_ctl on SL6.x i386/x86_64 (1801-1133)

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

Risk Level: Medium

CVE: CVE-2017-5715

Update Details

Risk is updated

175307 - Scientific Linux Security ERRATA Important: linux-firmware on SL7.x (noarch) (1801-1476)

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

Risk Level: Medium

CVE: CVE-2017-5715

Update Details

Risk is updated

175308 - Scientific Linux Security ERRATA Important: libvirt on SL6.x i386/x86_64 (1801-1816)

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

Risk Level: Medium

CVE: CVE-2017-5715

Update Details

Risk is updated

175309 - Scientific Linux Security ERRATA Important: microcode_ctl on SL7.x x86_64 (1801-433)

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

Risk Level: Medium

CVE: CVE-2017-5715

Update Details

Risk is updated

175310 - Scientific Linux Security ERRATA Important: qemu-kvm on SL6.x i386/x86_64 (1801-2147)

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

Risk Level: Medium

CVE: CVE-2017-5715

Update Details

Risk is updated

193109 - Fedora Linux 27 FEDORA-2017-1ebb87e7c0 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-17741

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.