

MCAFFEE 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

23042 - (HT208463) Apple iOS Multiple Vulnerabilities Prior To 11.2.5

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-2018-4082, CVE-2018-4085, CVE-2018-4086, CVE-2018-4087, CVE-2018-4088, CVE-2018-4089, CVE-2018-4090, CVE-2018-4092, CVE-2018-4093, CVE-2018-4094, CVE-2018-4095, CVE-2018-4096, CVE-2018-4100, CVE-2018-4109

Description

Multiple vulnerabilities are present in some versions of Apple iOS.

Observation

Apple iOS is the operating system used by Apple iPhone, iPad and iPod touch.

Multiple vulnerabilities are present in some versions of Apple iOS. The flaws lie in multiple components. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system, obtain restricted information or cause a denial of service condition.

23060 - (APSA18-01) Vulnerability In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2018-4878

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 lies in the Adobe Flash Player Runtime. Successful exploitation could allow an attacker to take control of the affected system.

23061 - (APSA18-01) Vulnerability In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2018-4878

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 lies in the Adobe Flash Player Runtime. Successful exploitation could allow an attacker to take control of the affected system.

23039 - (K02714910) F5 BIG-IP TLS Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2017-6164

Description

A vulnerability is present in some versions of F5's BIG-IP Products.

Observation

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

A vulnerability is present in some versions of F5's BIG-IP Products. The flaw lies in the Traffic Management Microkernel component. Successful exploitation could allow an attacker to cause a denial of service condition or remotely execute arbitrary code on the target system.

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.

193207 - Fedora Linux 27 FEDORA-2018-6349371aa1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-13194

Update Details

Risk is updated

22989 - WECON LeviStudio Multiple Buffer Overflow Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-16737, CVE-2017-16739

Update Details

Risk is updated

22993 - Oracle Java SE Critical Patch Update January 2018

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2581, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2627, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2638, CVE-2018-2639,

CVE-2018-2641, CVE-2018-2657, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

[Update Details](#)

Risk is updated

141839 - Red Hat Enterprise Linux RHSA-2018-0099 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2581, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2627, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2638, CVE-2018-2639, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

[Update Details](#)

Risk is updated

23023 - Oracle JRockit Critical Patch Update January 2018

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2588, CVE-2018-2599, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2637, CVE-2018-2657, CVE-2018-2663, CVE-2018-2678

[Update Details](#)

Risk is updated

130996 - Debian Linux 8.0, 9.0 DSA-4083-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000472

[Update Details](#)

Risk is updated

141846 - Red Hat Enterprise Linux RHSA-2018-0115 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2637, CVE-2018-2641, CVE-2018-2657, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

[Update Details](#)

Risk is updated

141850 - Red Hat Enterprise Linux RHSA-2018-0100 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2581, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2657, CVE-2018-2663, CVE-2018-2677,

CVE-2018-2678

[Update Details](#)

Risk is updated

141854 - Red Hat Enterprise Linux RHSA-2018-0095 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

[Update Details](#)

Risk is updated

146272 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0174-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5764

[Update Details](#)

Risk is updated

146274 - SuSE SLES 11 SP4 SUSE-SU-2018:0172-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5764

[Update Details](#)

Risk is updated

160349 - CentOS 6, 7 CESA-2018-0095 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

[Update Details](#)

Risk is updated

163534 - Oracle Enterprise Linux ELSA-2018-0095 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

[Update Details](#)

Risk is updated

175314 - Scientific Linux Security ERRATA Important: java-1.8.0-openjdk on SL6.x, SL7.x i386/x86_64 (1801-6612)

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

Risk Level: Medium

CVE: CVE-2018-2579, CVE-2018-2582, CVE-2018-2588, CVE-2018-2599, CVE-2018-2602, CVE-2018-2603, CVE-2018-2618, CVE-2018-2629, CVE-2018-2633, CVE-2018-2634, CVE-2018-2637, CVE-2018-2641, CVE-2018-2663, CVE-2018-2677, CVE-2018-2678

[Update Details](#)

Risk is updated

193214 - Fedora Linux 27 FEDORA-2018-ef9e28d9e4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000472

[Update Details](#)

Risk is updated

193230 - Fedora Linux 26 FEDORA-2018-7349a7723e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-1000472

[Update Details](#)

Risk is updated

HOW TO UPDATE

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

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

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

MCAFEE TECHNICAL SUPPORT

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

Multi-National Phone Support available here:

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

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

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by

others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2018 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates