

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

19468 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 38.5

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

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7205, CVE-2015-7210, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7222

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is an open source web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information, execute arbitrary code, cause a denial of service condition or bypass security measures.

19469 - Mozilla Firefox ESR Multiple Vulnerabilities Prior To 38.5

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7205, CVE-2015-7210, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7222

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is an open source web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox ESR. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information, execute arbitrary code, cause a denial of service condition or bypass security measures.

19470 - Mozilla Firefox Multiple Vulnerabilities Prior To 43

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

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7202, CVE-2015-7203, CVE-2015-7204, CVE-2015-7205, CVE-2015-7207, CVE-2015-7208, CVE-2015-7210, CVE-2015-7211, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7215, CVE-2015-7216, CVE-2015-7217, CVE-2015-7218, CVE-2015-7219, CVE-2015-7220, CVE-2015-7221, CVE-2015-7222, CVE-2015-7223

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information, execute arbitrary code, cause a denial of service condition or bypass security measures.

19471 - Mozilla Firefox Multiple Vulnerabilities Prior To 43

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-7201, CVE-2015-7202, CVE-2015-7203, CVE-2015-7204, CVE-2015-7205, CVE-2015-7207, CVE-2015-7208, CVE-2015-7210, CVE-2015-7211, CVE-2015-7212, CVE-2015-7213, CVE-2015-7214, CVE-2015-7215, CVE-2015-7216, CVE-2015-7217, CVE-2015-7218, CVE-2015-7219, CVE-2015-7220, CVE-2015-7221, CVE-2015-7222, CVE-2015-7223

Description

Multiple vulnerabilities are present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

Multiple vulnerabilities are present in some versions of Mozilla Firefox. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information, execute arbitrary code, cause a denial of service condition or bypass security measures.

19479 - (APSB16-01) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2015-8459, CVE-2015-8460, CVE-2015-8634, CVE-2015-8635, CVE-2015-8636, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8644, CVE-2015-8645, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, CVE-2015-8650, CVE-2015-8651

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

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

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws are due to type confusion, integer overflow, memory corruption and several use-after-free vulnerabilities. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB16-01 resolves these issues. The target system is missing this update.

19480 - (APSB16-01) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-8459, CVE-2015-8460, CVE-2015-8634, CVE-2015-8635, CVE-2015-8636, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8644, CVE-2015-8645, CVE-2015-8646, CVE-2015-8647,

CVE-2015-8648, CVE-2015-8649, CVE-2015-8650, CVE-2015-8651

Description

Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Observation

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

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws are due to type confusion, integer overflow, memory corruption and several use-after-free vulnerabilities. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB16-01 resolves these issues. The target system is missing this update.

19473 - Apache ActiveMQ Java Deserialization Vulnerability

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

Risk Level: High

CVE: CVE-2015-5254

Description

A vulnerability is present in some versions of Apache ActiveMQ.

Observation

Apache ActiveMQ is an open source messaging server.

A vulnerability is present in some versions of Apache ActiveMQ. The flaw is due to the usage of Java Serialization for marshalling or unmarshalling message payload. Successful exploitation could allow an attacker to remotely execute arbitrary code.

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.

141044 - Red Hat Enterprise Linux RHSA-2015-2665 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-6792

Update Details

Risk is updated

144099 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:2346-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-6792

Update Details

Risk is updated

181724 - FreeBSD chromium Multiple Vulnerabilities (bb7d4791-a5bf-11e5-a0e5-00262d5ed8ee)

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

Risk Level: High

CVE: CVE-2015-6792

[Update Details](#)

Risk is updated

130329 - Debian Linux 8.0 DSA-3411-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8327

[Update Details](#)

Risk is updated

185075 - Ubuntu Linux 12.04 USN-2831-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8327

[Update Details](#)

Risk is updated

185077 - Ubuntu Linux 14.04, 15.04, 15.10 USN-2831-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8327

[Update Details](#)

Risk is updated

91983 - Oracle Enterprise Linux ELSA-2015-2623 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

[Update Details](#)

Risk is updated

141039 - Red Hat Enterprise Linux RHSA-2015-2623 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

[Update Details](#)

Risk is updated

160008 - CentOS 7 CESA-2015-2653 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

Update Details

Risk is updated

185079 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2836-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

Update Details

Risk is updated

190089 - Fedora Linux 23 FEDORA-2015-cebe5133e7 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8370

Update Details

Risk is updated

190111 - Fedora Linux 23 FEDORA-2015-c59710b05d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-7446, CVE-2015-7550, CVE-2015-8543

Update Details

Risk is updated

190124 - Fedora Linux 22 FEDORA-2015-c1c2f5e168 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2013-7446, CVE-2015-7550, CVE-2015-8543

Update Details

Risk is updated

130334 - Debian Linux 7.0, 8.0 DSA-3420-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

[Update Details](#)

Risk is updated

130337 - Debian Linux 7.0, 8.0 DSA-3416-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8476

[Update Details](#)

Risk is updated

170601 - Amazon Linux AMI ALAS-2015-631 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

[Update Details](#)

Risk is updated

185080 - Ubuntu Linux 12.04, 14.04, 15.04, 15.10 USN-2837-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8000

[Update Details](#)

Risk is updated

19434 - (CTX203451) Citrix XenServer Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-8339, CVE-2015-8340

[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.

MCAFFEE 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 2015 McAfee, Inc.

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