2015-OCT-27
FSL version 7.5.757

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

19154 - Novell iPrint Appliance Multiple Vulnerabilities Prior To 1.1 Patch 3

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2013-6501, CVE-2013-7263, CVE-2013-7423, CVE-2014-0096, CVE-2014-0098, CVE-2014-0099, CVE-2014-0119, CVE-2014-0181, CVE-2014-0207, CVE-2014-0224, CVE-2014-0226, CVE-2014-0227, CVE-2014-0230, CVE-2014-0231, CVE-2014-0475, CVE-2014-0609, CVE-2014-1544, CVE-2014-1547, CVE-2014-1548, CVE-2014-1555, CVE-2014-1556, CVE-2014-1557, CVE-2014-1562, CVE-2014-1567, CVE-2014-1568, CVE-2014-1569, CVE-2014-1574, CVE-2014-1575, CVE-2014-1576, CVE-2014-1577, CVE-2014-1578, CVE-2014-1581, CVE-2014-1583, CVE-2014-1585, CVE-2014-1586, CVE-2014-1739, CVE-2014-2484, CVE-2014-2494, CVE-2014-2706, CVE-2014-3065, CVE-2014-3153, CVE-2014-3181, CVE-2014-3184, CVE-2014-3185, CVE-2014-3186, CVE-2014-3478, CVE-2014-3479, CVE-2014-3480, CVE-2014-3487, CVE-2014-3505, CVE-2014-3506, CVE-2014-3507, CVE-2014-3508, CVE-2014-3510, CVE-2014-3515, CVE-2014-3537, CVE-2014-3564, CVE-2014-3565, CVE-2014-3566, CVE-2014-3567, CVE-2014-3568, CVE-2014-3569, CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2014-3601, CVE-2014-3610, CVE-2014-3613, CVE-2014-3638, CVE-2014-3646, CVE-2014-3647, CVE-2014-3660, CVE-2014-3668, CVE-2014-3669, CVE-2014-3670, CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-3690, CVE-2014-3707, CVE-2014-3710, CVE-2014-4027, CVE-2014-4049, CVE-2014-4171, CVE-2014-4207, CVE-2014-4208, CVE-2014-4209, CVE-2014-4214, CVE-2014-4218, CVE-2014-4219, CVE-2014-4220, CVE-2014-4221, CVE-2014-4227, CVE-2014-4233, CVE-2014-4238, CVE-2014-4240, CVE-2014-4243, CVE-2014-4244, CVE-2014-4252, CVE-2014-4258, CVE-2014-4260, CVE-2014-4262, CVE-2014-4263, CVE-2014-4265, CVE-2014-4266, CVE-2014-4268, CVE-2014-4274, CVE-2014-4287, CVE-2014-4288, CVE-2014-4330, CVE-2014-4341, CVE-2014-4342, CVE-2014-4343, CVE-2014-4344, CVE-2014-4345, CVE-2014-4508, CVE-2014-4608, CVE-2014-4650, CVE-2014-4667, CVE-2014-4670, CVE-2014-4698, CVE-2014-4721, CVE-2014-4877, CVE-2014-4943, CVE-2014-5029, CVE-2014-5030, CVE-2014-5031, CVE-2014-5077, CVE-2014-5119, CVE-2014-5214

Description

Multiple vulnerabilities are present in some versions of Novell iPrint Appliance.

Observation

Novell iPrint Appliance is a popular virtual appliance that offers self-service printing for the enterprises.

Multiple vulnerabilities are present in some versions of Novell iPrint Appliance. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code.

19184 - (APSB15-26) Vulnerabilities In Adobe Shockwave Player

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

Risk Level: High

CVE: CVE-2015-7649

Description

A vulnerability is present in some versions of Adobe Shockwave Player.

Observation

Adobe Shockwave Player is a software used to view multimedia files created with Adobe Director.

A vulnerability is present in some versions of Adobe Shockwave Player. The flaw is due to a memory corruption error. Successful exploitation could allow an attacker to execute arbitrary code.

The update provided by Adobe bulletin APSB15-26 resolves the issue. The target system appears to be missing this update.

19155 - (JSA10700) Juniper Junos J-Web Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-6451

Description

A denial of service is present in some versions of Juniper Junos.

Observation

Juniper Junos is the operating system used in Juniper device.

A denial of service is present in some versions of Juniper Junos. The flaw lies in the J-Web service. Successful exploitation could allow an attacker to cause a denial of service condition.

19179 - Oracle MySQL Critical Patch Update October 2015

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

Risk Level: High

CVE: CVE-2015-1793, CVE-2015-4730, CVE-2015-4766, CVE-2015-4791, CVE-2015-4792, CVE-2015-4800, CVE-2015-4802, CVE-2015-4807, CVE-2015-4815, CVE-2015-4816, CVE-2015-4819, CVE-2015-4826, CVE-2015-4830, CVE-2015-4833, CVE-2015-4836, CVE-2015-4858, CVE-2015-4861, CVE-2015-4862, CVE-2015-4864, CVE-2015-4866, CVE-2015-4870, CVE-2015-4879, CVE-2015-4890, CVE-2015-4895, CVE-2015-4904, CVE-2015-4905, CVE-2015-4910, CVE-2015-4913

Description

Multiple vulnerabilities are present in some versions of Oracle MySQL Server.

Observation

Oracle MySQL Server is a popular open source database.

Multiple vulnerabilities are present in some versions of Oracle MySQL Server. The flaws lie in several components. Successful exploitation could allow an attacker to affect confidentiality, integrity and availability of the target system.

19159 - Novell eDirectory Multiple Vulnerabilities Prior To 8.8 SP8 Patch 6

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2012-5568

Description

A vulnerability is present in some versions of Novell (NetIQ) eDirectory.

Observation

Novell (NetIQ) eDirectory is an X.500 compatible directory service software for centrally managing access to network resources.

A vulnerability is present in some versions of Novell (NetIQ) eDirectory. The flaw lies in Apache Tomcat, used by the iMonitor component. Successful exploitation could allow an attacker to cause a denial of service condition.

19174 - (JSA10696) Juniper Junos TCP Reassembly Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-6449

Description

A vulnerability is present in some versions of Juniper Junos.

Observation

Juniper Junos is the operating system used in Juniper device.

A vulnerability is present in some versions of Juniper Junos. The flaw is due to improper handling of a very specific sequence of fragmented crafted packets. Successful exploitation could allow an attacker to cause a denial of service condition.

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.

130293 - Debian Linux 8.0 DSA-3373-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-4716, CVE-2015-4717, CVE-2015-4718, CVE-2015-5953, CVE-2015-5954, CVE-2015-6500, CVE-2015-6670, CVE-2015-7699

Update Details

Risk is updated

16432 - (HPSBMU02947) HP System Management Homepage Multiple Vulnerabilities Prior To 7.3

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

Risk Level: High

CVE: CVE-2013-4846, CVE-2013-6188

Update Details

Recommendation is updated

18740 - (SOL16912) F5 BIG-IP BIND Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-4620

Update Details

Documentation is updated

18743 - (SOL16909) F5 BIG-IP BIND Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-5477

Update Details

Documentation is updated

18903 - VideoLAN VLC Media Player 3GP File Arbitrary Pointer Dereference Vulnerability

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

Risk Level: High

CVE: CVE-2015-5949

Update Details

Recommendation is updated

19083 - PostgreSQL Multiple Vulnerabilities (Oct 2015)

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

Risk Level: Medium

CVE: CVE-2015-5288, CVE-2015-5289

Update Details

Risk is updated

130294 - Debian Linux 8.0 DSA-3374-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288, CVE-2015-5289

Update Details

Risk is updated

181629 - FreeBSD PostgreSQL Minor Security Problems. (a0182578-6e00-11e5-a90c-0026551a22dc)

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

Risk Level: Medium

CVE: CVE-2015-5288, CVE-2015-5289

Update Details

Risk is updated

185022 - Ubuntu Linux 12.04, 14.04, 15.04 USN-2772-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5288, CVE-2015-5289

Update Details

Risk is updated

18721 - (SOL16898) F5 BIG-IP PKCS #7 Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-1790

Update Details

Documentation is updated

70032 - mysql.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.

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