2016-APR-19
FSL version 7.5.814

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

19947 - IBM WebSphere Portal Multiple Oracle Outside In Technology Vulnerabilities (swg21975750)

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

Risk Level: High

CVE: CVE-2015-4808, CVE-2015-4809, CVE-2015-4811, CVE-2015-4877, CVE-2015-4878, CVE-2015-6013, CVE-2015-6014, CVE-2015-6015, CVE-2016-0432

Description

Multiple vulnerabilities are present in some versions of IBM WebSphere Portal.

Observation

IBM WebSphere Portal is a set of software tools that is used to build and manage web portals.

Multiple vulnerabilities are present in some versions of IBM WebSphere Portal. The flaws lie in the Oracle Outside In Technology component. Successful exploitation could allow an attacker to execute arbitrary code or to cause a denial of service.

19962 - Oracle Java SE Critical Patch Update April 2016

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

Risk Level: High

CVE: CVE-2016-0686, CVE-2016-0687, CVE-2016-0695, CVE-2016-3422, CVE-2016-3425, CVE-2016-3426, CVE-2016-3427, CVE-2016-3443, CVE-2016-3449

Description

Multiple vulnerabilities are present in some versions of Oracle Java SE.

Observation

Oracle Java SE is used to run Java applications.

Multiple vulnerabilities are present in some versions of Oracle Java SE. The flaws lie in multiple components. Successful exploitation could allow an attacker to obtain sensitive information, cause denial of service condition or execute arbitrary code.

19879 - (SOL81903701) F5 BIG-IP Libpng Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-8472

Description

A vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the libpng library. Successful exploitation could allow an attacker to cause a denial of service condition or possibly have other unspecified impact in the target system.

19881 - (SOL95698826) F5 BIG-IP LZO Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-4607

Description

A vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the LZO library. Successful exploitation could allow an attacker to cause a denial of service condition or to remotely execute arbitrary code.

19883 - (SOL63519101) F5 BIG-IP QEMU Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2014-8106, CVE-2015-3209, CVE-2015-5165, CVE-2015-5279, CVE-2015-7504, CVE-2015-7512

Description

Multiple vulnerabilities are present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

Multiple vulnerabilities are present in some versions of F5 BIG-IP products. The flaws lie in the QEMU component. Successful exploitation could allow an attacker to cause a denial of service condition, to retrieve sensitive data or to remotely execute arbitrary code.

19872 - (SOL50413110) F5 BIG-IP GnuPG Security Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-4351

Description

A security bypass vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A security bypass vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in how the GnuPG component handles key flags subpackets. Successful exploitation could allow an attacker to bypass system security mechanisms.

19874 - (SOL11785283) F5 BIG-IP GnuPG Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2012-6085

Description

A vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the GnuPG component, specifically in the read_block function. Successful exploitation could allow an attacker to cause a denial of service condition.

19877 - (SOL98102572) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7990

Description

A vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the Linux kernel. Successful exploitation could allow an attacker to cause a denial of service condition or possibly have other unspecified impact in the target system. This is a locally exploitable vulnerability.

19871 - (SOL40131068) F5 BIG-IP GnuPG Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-4402

Description

A denial of service vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A denial of service vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the compressed packet parser in GnuPG component. Successful exploitation could allow an attacker to cause a denial of service condition.

19876 - (SOL20022580) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-7446

Description

A vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the Linux kernel. Successful exploitation could allow an attacker to cause a denial of service condition or to bypass security access restrictions. This is a locally exploitable vulnerability.

19880 - (SOL15095307) F5 BIG-IP BDF Parsing Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2012-5669

Description

A vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the FreeType component. Successful exploitation could allow an attacker to cause a denial of service condition or to remotely execute arbitrary code.

19884 - (SOL21057235) F5 BIG-IP Libpng Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7981

Description

An information disclosure vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

An information disclosure vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the libpng component, specifically in the png_convert_to_rfc1123 function. Successful exploitation could allow an attacker to retrieve sensitive data.

19875 - (SOL71245322) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-8138

Description

A vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the NTP component. Successful exploitation could allow an attacker to disable time synchronization or to alter the time on the target system through crafted NTP packets.

19882 - (SOL19157044) F5 BIG-IP Libtirpc Denial Of Service Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2013-1950

Description

A vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

A vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the libtirpc component. Successful exploitation could allow an attacker to cause a denial of service condition.

19950 - Dell iDRAC Path Traversal Authentication Bypass Vulnerability

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

Risk Level: Low

CVE: CVE-2015-7270

Description

A directory traversal vulnerability is present in some versions of Dell Integrated Dell Remote Access Controller.

Observation

Dell Integrated Dell Remote Access Controller is a popular embedded server management solution.

A directory traversal vulnerability is present in some versions of Dell Integrated Dell Remote Access Controller. The flaw lies in an unknown component of Dell Integrated Dell Remote Access Controller. Successful exploitation could allow an attacker to log into the system bypassing security measures.

19873 - (SOL75253136) F5 BIG-IP GnuPG Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2013-4242

Description

An information disclosure vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

An information disclosure vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the GnuPG component. Successful exploitation could allow an attacker to retrieve sensitive data. This is a locally exploitable vulnerability.

19878 - (SOL60742457) F5 BIG-IP Linux Kernel Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2015-8374

Description

An information disclosure vulnerability is present in some versions of F5 BIG-IP products.

Observation

F5's BIG-IP product is a network appliance that runs F5's Traffic Management Operating System.

An information disclosure vulnerability is present in some versions of F5 BIG-IP products. The flaw lies in the Linux kernel. Successful exploitation could allow an attacker to retrieve sensitive data from the target system. This is a locally exploitable vulnerability.

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.

19705 - SAP 3D Visual Enterprise Viewer SketchUp Document Multiple Use-After-Free Remote Code Execution Vulnerabilities

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

13749 - Apple iOS Safari match() Buffer Denial of Service

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated Documentation is updated

13986 - Apple iOS Safari match() Buffer Denial of Service

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated Documentation is updated

19708 - Netgear Management System NMS300 Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2016-1524, CVE-2016-1525

Update Details

Recommendation is updated

937 - Apple Airport Base Station WEP Key Disclosure

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

19725 - (SA-CORE-2016-001) Drupal Core Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2016-3162, CVE-2016-3163, CVE-2016-3164, CVE-2016-3165, CVE-2016-3166, CVE-2016-3167, CVE-2016-3168, CVE-2016-3169, CVE-2016-3170, CVE-2016-3171

Update Details

CVE is updated

38209 - Apple Mac OS X XNU Kernel Memory Denial-of-Service Vulnerability

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2009-1237

Update Details

Recommendation is updated Documentation 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.