2016-OCT-26
FSL version 7.5.860

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

20711 - (JSA10759) Juniper Junos OpenSSL March 2016 Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-0702, CVE-2016-0703, CVE-2016-0704, CVE-2016-0705, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799

Description

Multiple vulnerabilities are present in some versions of Juniper JunOS.

Observation

Juniper JunOS is an operating system used in Juniper devices.

Multiple vulnerabilities are present in some versions of Juniper JunOS. The flaws lie in the OpenSSL component. Successful exploitation could allow an attacker to retrieve sensitive data or cause a denial of service condition.

20712 - (JSA10759) Juniper Junos OpenSSL May 2016 Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176, CVE-2016-2180

Description

Multiple vulnerabilities are present in some versions of Juniper JunOS.

Observation

Juniper JunOS is an operating system used in Juniper devices.

Multiple vulnerabilities are present in some versions of Juniper JunOS. The flaws lie in the OpenSSL component. Successful exploitation could allow an attacker to retrieve sensitive data or cause a denial of service condition.

20724 - Cisco Nexus 7000 and 7700 Series Switches Overlay Transport Virtualization Buffer Overflow Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1453

Description

A buffer overflow vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is the operating system used in Cisco Nexus devices.

A buffer overflow vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in the processing of OTV packet header parameters. Successful exploitation could allow an attacker to cause a denial of service condition or execute arbitrary code.

20726 - Oracle MySQL Server Critical Patch Update October 2016

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

Risk Level: High

CVE: CVE-2016-3492, CVE-2016-3495, CVE-2016-5507, CVE-2016-5584, CVE-2016-5609, CVE-2016-5612, CVE-2016-5616, CVE-2016-5617, CVE-2016-5624, CVE-2016-5625, CVE-2016-5626, CVE-2016-5627, CVE-2016-5628, CVE-2016-5629, CVE-2016-5630, CVE-2016-5631, CVE-2016-5632, CVE-2016-5633, CVE-2016-5634, CVE-2016-5635, CVE-2016-6304, CVE-2016-6662, CVE-2016-7440, CVE-2016-8283, CVE-2016-8284, CVE-2016-8286, CVE-2016-8287, CVE-2016-8288, CVE-2016-8289, CVE-2016-8290

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 the following server components: Logging, Error Handling, Packaging, DML, GIS, InnoDB, Optimizer, Federated, Memcached, Performance Schema, RBR, Replication, Types and other security components. OpenSSL subcomponent is also affected. Successful exploitation could allow an attacker to cause a denial of service condition, retrieve sensitive data, do unauthorized modifications or conduct a takeover attack on the target system.

20729 - Oracle WebLogic Server Critical Patch Update October 2016

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

Risk Level: High

CVE: CVE-2015-7501, CVE-2016-3505, CVE-2016-5488, CVE-2016-5531, CVE-2016-5535, CVE-2016-5601

Description

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

Observation

Oracle WebLogic Server is a Java EE application server.

Multiple vulnerabilities are present in some versions of Oracle WebLogic Server. The flaws lie in multiple components. Successful exploitation could allow an attacker to execute arbitrary code, cause a denial of service condition or retrieve sensitive data.

20733 - (JSA10759) Juniper ScreenOS OpenSSL Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-0797, CVE-2016-0800, CVE-2016-2105, CVE-2016-2106, CVE-2016-2108

Description

Multiple vulnerabilities are present in some versions of Juniper ScreenOS.

Observation

Juniper ScreenOS is a popular firewall and VPN operating system.

Multiple vulnerabilities are present in some versions of Juniper ScreenOS. The flaws lie in the OpenSSL component. Successful exploitation could allow an attacker to execute remote code, disclose information or cause a denial of service condition.

20740 - (APSB16-36) Vulnerability In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2016-7855

Description

A vulnerability is 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.

A vulnerability is present in some versions of Adobe Flash Player. The flaw occurs due to a memory issue. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB16-36 resolves the issue. The target system is missing this update.

20741 - (APSB16-36) Vulnerability In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-7855

Description

A vulnerability is 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.

A vulnerability is present in some versions of Adobe Flash Player. The flaw occurs due to a memory issue. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB16-36 resolves the issue. The target system is missing this update.

20725 - Oracle VM VirtualBox Critical Patch Update October 2016

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

Risk Level: High

CVE: CVE-2016-5501, CVE-2016-5538, CVE-2016-5605, CVE-2016-5608, CVE-2016-5610, CVE-2016-5611, CVE-2016-5613, CVE-2016-6304

Description

Multiple vulnerabilities are present in some versions of Oracle VM VirtualBox.

Observation

Oracle VM VirtualBox is a virtualization software.

Multiple vulnerabilities are present in some versions of Oracle VM VirtualBox. The flaws exist in the VirtualBox Remote Desktop

Extension (VRDE) and Core components. Successful exploitation could allow an attacker to cause a denial of service condition, retrieve sensitive data or do unauthorized modifications on the target system.

20714 - Google Chrome Multiple Vulnerabilities Prior To 54.0.2840.59

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

Risk Level: High

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193, CVE-2016-5194

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular Internet browser.

Multiple vulnerabilities are present in some versions of Google Chrome. These flaws lie in multiple components. Successful exploitation could allow an attacker to launch spoofing attack, obtain sensitive information, bypass certain security restrictions.

20715 - Google Chrome Multiple Vulnerabilities Prior To 54.0.2840.59

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-5181, CVE-2016-5182, CVE-2016-5183, CVE-2016-5184, CVE-2016-5185, CVE-2016-5186, CVE-2016-5187, CVE-2016-5188, CVE-2016-5189, CVE-2016-5190, CVE-2016-5191, CVE-2016-5192, CVE-2016-5193, CVE-2016-5194

Description

Multiple vulnerabilities are present in some versions of Google Chrome.

Observation

Google Chrome is a popular Internet browser.

Multiple vulnerabilities are present in some versions of Google Chrome. These flaws lie in multiple components. Successful exploitation could allow an attacker to launch spoofing attack, obtain sensitive information, bypass certain security restrictions.

20716 - (JSA10762) Juniper Junos IPv6 Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-4921

Description

A denial of service vulnerability is present in some versions of Juniper JunOS.

Observation

Juniper JunOS is an operating system used in Juniper devices.

A denial of service vulnerability is present in some versions of Juniper JunOS. The flaw lies in the IPv6 traffic management. Successful exploitation could allow an attacker to cause a denial of service condition.

20718 - (HT207147) Apple iCloud WebKit Memory Corruption Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2016-4762

Description

A memory corruption vulnerability is present in some versions of Apple iCloud.

Observation

Apple iCloud is a manager for the Apple's cloud-based storage service.

A memory corruption vulnerability is present in some versions of Apple iCloud. The flaw lies in Apple iCloud's WebKit component. Successful exploitation could allow an attacker to execute arbitrary code, retrieve sensitive data or cause a denial of service condition.

20722 - Cisco NX-OS Border Gateway Protocol Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-1454

Description

A denial of service vulnerability is present in some versions of Cisco NX-OS Software.

Observation

Cisco NX-OS Software is an operating system used in Cisco Nexus devices.

A denial of service vulnerability is present in some versions of Cisco NX-OS Software. The flaw lies in Border Gateway Protocol (BGP) implementation. Successful exploitation could allow an attacker to cause the target reload.

20720 - (HT207263) Apple iOS Multiple Vulnerabilities Prior To 10.0.3

Category: Wireless Assessment -> NonIntrusive -> iOS

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

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 attackers to have other impacts on iOS devices.

20574 - (SOL02201365) F5 BIG-IP SLOTH: TLS 1.2 Handshake Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-7575

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 the TLS 1.2 handshakes. Successful exploitation could allow an attacker to spoof the servers.

20719 - (CTX217363) Citrix XenServer Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Low

CVE: CVE-2016-7777

Description

A vulnerability is present in some versions of Citrix XenServer.

Observation

Citrix XenServer is a popular virtualization platform.

A vulnerability is present in some versions of Citrix XenServer. The flaw is related to the CR0.TS and CR0.EM register flags. Successful exploitation could allow an attacker to retrieve or modify data 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.

82233 - FreeBSD openSSL Multiple Problems In Crypto(3) (0f37d765-c5d4-11db-9f82-000e0c2e438a)

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

Risk Level: High

CVE: CVE-2006-2937, CVE-2006-2940, CVE-2006-3738, CVE-2006-4343

Update Details

CVE is updated

144777 - SuSE SLES 11 SP4 SUSE-SU-2016:1996-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-3205, CVE-2011-4096, CVE-2012-5643, CVE-2013-0189, CVE-2013-4115, CVE-2014-0128, CVE-2014-6270, CVE-2014-7141, CVE-2014-7142, CVE-2015-5400, CVE-2016-2390, CVE-2016-2569, CVE-2016-2570, CVE-2016-2571, CVE-2016-2572, CVE-2016-3947, CVE-2016-3948, CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4553, CVE-2016-4554, CVE-2016-4555, CVE-2016-4556

Update Details

CVE is updated

144797 - SuSE SLES 11 SP4 SUSE-SU-2016:2089-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2011-3205, CVE-2011-4096, CVE-2012-5643, CVE-2013-0189, CVE-2013-4115, CVE-2014-0128, CVE-2014-6270, CVE-2014-7141, CVE-2014-7142, CVE-2015-5400, CVE-2016-2390, CVE-2016-2569, CVE-2016-2570, CVE-2016-2571, CVE-2016-2572,

CVE-2016-3947, CVE-2016-3948, CVE-2016-4051, CVE-2016-4052, CVE-2016-4053, CVE-2016-4054, CVE-2016-4553, CVE-2016-4554, CVE-2016-4555, CVE-2016-4556

Update Details

CVE is updated

130500 - Debian Linux 8.0 DSA-3584-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7558, CVE-2016-4348

Update Details

CVE is updated

88800 - Slackware Linux 14.2 SSA:2016-236-03 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5696

Update Details

CVE is updated

88801 - Slackware Linux 14.1 SSA:2016-242-01 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2016-5696

Update Details

CVE is updated

70017 - cisco.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.