2016-DEC-02
FSL version 7.5.869

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

20936 - Mozilla Firefox ESR SVG Animation Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2016-9079

Description

A use-after-free vulnerability is present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

A use-after-free vulnerability is present in some versions of Mozilla Firefox ESR. The flaw lies in SVG Animation. Successful exploitation could allow an attacker to remotely execute arbitrary code.

20937 - Mozilla Firefox ESR SVG Animation Remote Code Execution Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-9079

Description

A use-after-free vulnerability is present in some versions of Mozilla Firefox ESR.

Observation

Mozilla Firefox ESR is a popular web browser.

A use-after-free vulnerability is present in some versions of Mozilla Firefox ESR. The flaw lies in SVG Animation. Successful exploitation could allow an attacker to remotely execute arbitrary code.

20916 - (SOL93122894) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2016-0705

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 OpenSSL component. Successful exploitation could allow an attacker to cause a denial of service condition or possibly have other unspecified impact in the target system.

20938 - Mozilla Firefox SVG Animation Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2016-9079

Description

A use-after-free vulnerability is present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

A use-after-free vulnerability is present in some versions of Mozilla Firefox. The flaw lies in SVG Animation. Successful exploitation could allow an attacker to execute arbitrary code.

20939 - Mozilla Firefox SVG Animation Remote Code Execution Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-9079

Description

A use-after-free vulnerability is present in some versions of Mozilla Firefox.

Observation

Mozilla Firefox is a popular web browser.

A use-after-free vulnerability is present in some versions of Mozilla Firefox. The flaw lies in SVG Animation. Successful exploitation could allow an attacker to execute arbitrary code.

20930 - (SOL51079478) F5 BIG-IP glibc Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-8778

Description

An integer overflow vulnerabilities are present in glibc (GNU C Library) in some versions of F5 BIG-IP systems.

Observation

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

An integer overflow vulnerabilities are present in glibc (GNU C Library) in some versions of F5 BIG-IP systems. The flaw is due to improper size check in the hcreate functions in glibc. Successful exploitation could allow remote attackers to cause a denial of service or arbitrary code execution on the affected systems.

20929 - (HPSBHF03675) HPE Integrated Lights-Out Cross-Site Scripting Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-4406

Description

A Cross-Site Scripting vulnerability is present in some versions of HP Integrated Lights-Out.

Observation

HP Integrated Lights-Out is a Hewlett-Packard proprietary embedded server management technology.

A Cross-Site Scripting vulnerability is present in some versions of HP Integrated Lights-Out. The flaw lies in an unknown component. Successful exploitation could allow a remote attacker to execute arbitrary code.

20910 - (SOL51518670) F5 BIG-IP Linux Kernel Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-2922

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 Linux Kernel component. Successful exploitation could allow a local attacker to cause a denial of service condition.

20912 - (SOL79215841) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2016-0702

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 OpenSSL component. Successful exploitation could allow a local attacker to retrieve sensitive data.

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.

16831 - 3S Software CoDeSys ENI Server Stack Buffer Overflow Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

20471 - (SOL20225390) F5 BIG-IP Multiple PCRE Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: High

CVE: CVE-2015-2327, CVE-2015-2328, CVE-2015-3217, CVE-2015-8380, CVE-2015-8381, CVE-2015-8382, CVE-2015-8383, CVE-2015-8384, CVE-2015-8385, CVE-2015-8386, CVE-2015-8387, CVE-2015-8388, CVE-2015-8389, CVE-2015-8390, CVE-2015-8391, CVE-2015-8392, CVE-2015-8394, CVE-2015-8395

Update Details

Recommendation is updated

8872 - Callisto PhotoParade Player PhPInfo ActiveX Control Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2007-1688

Update Details

Recommendation is updated

13383 - Beckhoff TwinCAT TCatScopeView SVW And SCP File Processing Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

4207 - BLNews Path Parameter Vulnerability

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

Risk Level: High

CVE: CVE-2003-0394

Update Details

Recommendation is updated

20443 - (SOL30971148) F5 BIG-IP Apache Tomcat Vulnerabilities

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-5174, CVE-2015-5345, CVE-2016-0706, CVE-2016-0714

Update Details

Recommendation is updated

18111 - B&B Electronics Vlinx ConnectPro Manager Remote Denial of Service

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

20587 - (SOL05428062) F5 BIG-IP Pcregrep In PCRE Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-8393

Update Details

Documentation is updated

4299 - BroadVision One-To-One Enterprise Information Disclosure

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

Risk Level: Medium

CVE: CVE-2001-0031

Update Details

Recommendation is updated

19875 - (SOL71245322) F5 BIG-IP NTP Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Medium

CVE: CVE-2015-8138

Update Details

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.