2017-FEB-21
FSL version 7.5.893

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

21272 - Hanwha Techwin Smart Security Manager Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-5168, CVE-2017-5169

Description

Multiple vulnerabilities are present in some versions of Hanwha Techwin Smart Security Manager.

Observation

Hanwha Techwin Smart Security Manager is a complete video management software platform.

Multiple vulnerabilities are present in some versions of Hanwha Techwin Smart Security Manager. The flaws lie in the ActiveMQ Broker service, the Redis and Apache Felix Gogo servers. Successful exploitation could allow a remote attacker to execute arbitrary code.

21279 - Sielco Sistemi Winlog DLL Hijacking Vulnerability

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

Risk Level: High

CVE: CVE-2017-5161

Description

A vulnerability is present in some versions of Sielco Sistemi Winlog.

Observation

Sielco Sistemi Winlog is a SCADA/HMI application development platform.

A vulnerability is present in some versions of Sielco Sistemi Winlog. The flaw is due to an uncontrolled search path element. Successful exploitation could allow an attacker to conduct hijacking attacks and escalate privileges on the target system.

21281 - (K43570545) F5 BIG-IP OpenSSL Vulnerability

Category: SSH Module -> NonIntrusive -> F5

Risk Level: Low

CVE: CVE-2016-7055

Description

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

Observation

F5's BIG-IP products are network appliances that run 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 OpenSSL Component. Successful exploitation could allow an attacker to cause a denial of service condition.

21287 - IBM WebSphere Application Server Potential Cross-Site Scripting Vulnerability (swg21997743)

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

Risk Level: Low

CVE: CVE-2017-1121

Description

A cross-site scripting vulnerability is present in some versions of IBM WebSphere Application Server.

Observation

IBM WebSphere Application Server is a Java application server.

A cross-site scripting vulnerability is present in some versions of IBM WebSphere Application Server. The flaw lies in Admin Console. Successful exploitation could allow an attacker to execute arbitrary JavaScript code, leading to credentials disclosure within a trusted session.

21294 - Windows gdi32.dll Information Disclosure Vulnerability

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

Risk Level: Low

CVE: CVE-2017-0038

Description

An information disclosure vulnerability is present in some versions of Microsoft Windows.

Observation

Microsoft Windows is a popular operating system.

An information disclosure vulnerability is present in some versions of Microsoft Windows. The flaws lie in the Windows Graphics Device Interface (gdi32.dll). Successful exploitation could allow a malicious user to obtain sensitive information.

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.

70116 - scada.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.