2013-NOV-06

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

15839 - Apple Remote Desktop Unencrypted Connection Security Issue and Format String Vulnerability

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

Risk Level: High

CVE: CVE-2013-5135, CVE-2013-5136

Description

Multiple vulnerabilities are present in some versions of Apple Remote Desktop.

Observation

Apple Remote Desktop is a suite of integrated desktop management tools.

Multiple vulnerabilities are present in some versions of Apple Remote Desktop. The flaws lie in the handling of the VNC username and authentication types. Successful exploitation could allow an attacker to execute arbitrary code.

15863 - Microsoft Graphics Component Remote Code execution

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3906

Microsoft KB: 2896666

Description

A remote code execution vulnerability is present in some versions of multiple Microsoft products.

Observation

A remote code execution vulnerability is present in some versions of multiple Microsoft products.

The flaw lies in the handling of TIFF images by the Graphics component that is present in versions of Windows, Office and Lync. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious file of visit a malicious website.

15825 - Oracle Virtualization Oracle Secure Global Desktop ttaauxserv Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-3834

DISA IAVA: 2013-A-0195

Description

A denial of service vulnerability is present in some versions of Oracle Virtualization.

Observation

A denial of service vulnerability is present in some versions of Oracle Virtualization.

The flaw lies in the ttaauxserv sub-component. Successful exploitation by a remote attacker could result in a denial of service condition.

15829 - Cisco NX-OS BGP Component Invalid AS Path Value Handling Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2012-4099

Description

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

Observation

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

The flaw is due to improper filtering of invalid AS Path values. Successful exploitation by a remote attacker could result in a denial of service condition.

15838 - WellinTech KingView SuperGrid and KChartXY ActiveX Path Traversal Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2013-6127, CVE-2013-6128

Description

Multiple path traversal vulnerabilities are present in some versions of WellinTech KingView.

Observation

WellinTech KingView is a SCADA software.

Multiple path traversal vulnerabilities are present in some versions of WellinTech KingView. The flaw lies in KChartXY.ocx and SuperGrid.ocx ActiveX control. Successful exploitation could allow an attacker to traverse outside a restricted path.

15847 - Cisco ASA Clientless SSL VPN Rewriter Denial of Service Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-5551

Description

A stack overflow vulnerability is present in some versions of Cisco ASA.

Observation

Cisco ASA is an operating system used in Cisco Firewall devices.

A stack overflow vulnerability is present in some versions of Cisco ASA. The flaw lies in the clientless SSL VPN feature.

Successful exploitation could allow an attacker to cause a denial of service.

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.

3933 - Cisco IP Phone Information Disclosure

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

Risk Level: High

Check Version: 1.1

Update Details

Observation is updated.
Recommendation is updated.

14264 - Oracle Java SE Multiple Vulnerabilities Prior To 7 Update 9

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

Risk Level: High

CVE: CVE-2012-1532, CVE-2012-1533, CVE-2012-3143, CVE-2012-3159, CVE-2012-3216, CVE-2012-4416, CVE-2012-5067, CVE-2012-5068, CVE-2012-5069, CVE-2012-5070, CVE-2012-5071, CVE-2012-5072, CVE-2012-5073, CVE-2012-5074, CVE-2012-5075, CVE-2012-5076, CVE-2012-5077, CVE-2012-5079, CVE-2012-5081, CVE-2012-5083, CVE-2012-5084, CVE-2012-5085, CVE-2012-5086, CVE-2012-5087, CVE-2012-5088, CVE-2012-5089

DISA IAVA: 2012-A-0171

Update Details

CVE is updated.

15689 - Mitsubishi MC-WorkX IcoLaunch ActiveX Control Remote Code Execution Vulnerability

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

Risk Level: High

Update Details

Recommendation is updated.

13240 - Bugzilla Unauthorized Account Creation Vulnerability (CVE-2011-3667)

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

Risk Level: Medium

CVE: CVE-2011-3667

Update Details

Recommendation is updated.

14874 - Oracle MySQL Server Geometry Query Processing Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-2013-1861

Update Details

Recommendation is updated.

15600 - TP-LINK TD-W8951ND Router Cross-Site Scripting and Request Forgery Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

Update Details

Recommendation is updated.

15628 - Wireshark Multiple Vulnerabilities Prior To 1.10.2

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

Risk Level: Medium

CVE: CVE-2013-4933, CVE-2013-5717, CVE-2013-5718, CVE-2013-5719, CVE-2013-5720, CVE-2013-5721, CVE-2013-5722, CVE-2013-6338

DISA IAVA: 2013-B-0105

Update Details

CVE is updated.

15629 - Wireshark Multiple Vulnerabilities Prior To 1.8.10

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

Risk Level: Medium

CVE: CVE-2013-4933, CVE-2013-5718, CVE-2013-5719, CVE-2013-5720, CVE-2013-5721, CVE-2013-5722, CVE-2013-6338

DISA IAVA: 2013-B-0105

Update Details

CVE 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.