2014-DEC-09
FSL version 7.5.653

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

17485 - (MS14-081) Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow (3017301)

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

Risk Level: High

CVE: CVE-2014-6356 , CVE-2014-6357

Description

Multiple vulnerabilities are present in some versions of Microsoft Office.

Observation

Microsoft Office is a popular office suite.

Multiple vulnerabilities are present in some versions of Microsoft Office. The flaws are due to Microsoft Word does not properly handle objects in memory while parsing specially crafted Office files. Successful exploitation could allow an attacker to execute remote code.

Microsoft has provided MS14-081 to address these issues. The host appears to be missing this patch.

17486 - (MS14-081) Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow (3017301)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-6356 , CVE-2014-6357

Description

Multiple vulnerabilities are present in some versions of Microsoft Office.

Observation

Microsoft Office is a popular office suite.

Multiple vulnerabilities are present in some versions of Microsoft Office. The flaws are due to Microsoft Word does not properly handle objects in memory while parsing specially crafted Office files. Successful exploitation could allow an attacker to execute remote code.

Microsoft has provided MS14-081 to address these issues. The host appears to be missing this patch.

17487 - (MS14-083) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (3017347)

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

Risk Level: High

CVE: CVE-2014-6360 , CVE-2014-6361

Description

Multiple vulnerabilities are present in some versions of Microsoft Excel.

Observation

Microsoft Excel is a popular spreadsheet application.

Multiple vulnerabilities are present in some versions of Microsoft Excel. The flaws are due to Microsoft Excel does not properly handle objects in memory while parsing specially crafted Office files. Successful exploitation could allow an attacker to execute remote code.

Microsoft has provided MS14-083 to address these issues. The host appears to be missing this patch.

17484 - (MS14-084) Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3016711)

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

Risk Level: High

CVE: CVE-2014-6363

Description

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

Observation

Microsoft Windows VBScript scripting engines are responsible for parsing and executing VBScript code.

A remote code execution vulnerability is present in some versions of Microsoft VBScript. The flaw lies in the handling of objects in memory. Successful exploitation could allow an attacker to execute remote code.

Microsoft has provided MS14-084 to address this issue. The host appears to be missing this patch.

17488 - (MS14-081) Microsoft Word Index Remote Code Execution (3017301)

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

Risk Level: High

CVE: CVE-2014-6356

Description

A vulnerability in some versions of Microsoft Word could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Word could lead to remote code execution.

The flaw lies in the handling of specially crafted Office files. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17489 - (MS14-081) Microsoft Word Use-After-Free Remote Code Execution (3017301)

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

Risk Level: High

CVE: CVE-2014-6357

Description

A vulnerability in some versions of Microsoft Word could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Word could lead to remote code execution.

The flaw lies in the handling of specially crafted Office files. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17495 - (MS14-084) Microsoft VBScript Memory Corruption Remote Code Execution (3016711)

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

Risk Level: High

CVE: CVE-2014-6363

Description

A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft VBScript could lead to remote code execution.

The flaw exists in the way that the VBScript engine, when rendered in Internet Explorer, handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17498 - (MS14-080) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6327

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

The flaw lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17499 - (MS14-080) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6329

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

The flaw lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17500 - (MS14-080) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6330

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

The flaw lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17501 - (MS14-080) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6366

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

The flaw lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17502 - (MS14-080) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6369

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

The flaw lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17503 - (MS14-080) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6373

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

The flaw lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17504 - (MS14-080) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6374

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

The flaw lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17505 - (MS14-080) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6375

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

The flaw lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17506 - (MS14-080) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6376

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

The flaw lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17507 - (MS14-080) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-8966

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

The flaw lies in a memory corruption error. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17508 - (MS14-080) Microsoft Internet Explorer VBScript Memory Corruption Remote Code Execution (3008923)

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

Risk Level: High

CVE: CVE-2014-6363

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to remote code execution.

The flaw lies in the VBScript component. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a vulnerable website, email or document.

17517 - (APSB14-27) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2014-0580, CVE-2014-0587, CVE-2014-8443, CVE-2014-9162, CVE-2014-9163, CVE-2014-9164

Description

Multiple vulnerabilities are 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.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB14-27 resolves these issues. The target system is missing this update.

17518 - (APSB14-27) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-0580, CVE-2014-0587, CVE-2014-8443, CVE-2014-9162, CVE-2014-9163, CVE-2014-9164

Description

Multiple vulnerabilities are 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.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws lie in several components. Successful exploitation could allow an attacker to execute remote code.

The update provided by Adobe bulletin APSB14-27 resolves these issues. The target system is missing this update.

17519 - (APSB14-28) Vulnerabilities in Adobe Reader and Acrobat

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

Risk Level: High

CVE: CVE-2014-8445, CVE-2014-8446, CVE-2014-8447, CVE-2014-8448, CVE-2014-8449, CVE-2014-8451, CVE-2014-8452, CVE-2014-8453, CVE-2014-8454, CVE-2014-8455, CVE-2014-8456, CVE-2014-8457, CVE-2014-8458, CVE-2014-8459, CVE-2014-8460, CVE-2014-8461, CVE-2014-9150, CVE-2014-9158, CVE-2014-9159, CVE-2014-9165

Description

Multiple vulnerabilities are present in some versions of Adobe Reader and Acrobat.

Observation

Adobe Reader and Acrobat are two popular software used to handle PDF files.

Multiple vulnerabilities are present in some versions of Adobe Reader and Acrobat. The flaws occur due to multiple memory corruption issues. Successful exploitation could allow an attacker to remotely execute arbitrary code.

The update provided by Adobe bulletin APSB14-28 resolves these issues. The target system appears to be missing this update.

17483 - (MS14-082) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3017349)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6364

Description

Multiple vulnerabilities are present in some versions of Microsoft Office.

Observation

Microsoft Office is a popular office suite.

Multiple vulnerabilities are present in some versions of Microsoft Office. The flaws exist in the Microsoft Office shared components which does not properly handle objects in memory while parsing specially crafted Office files. Successful exploitation could allow an attacker to execute remote code. The exploit requires the user to open a malicious Word document.

Microsoft has provided MS14-082 to address these issues. The host appears to be missing this patch.

17401 - (MS14-075) Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege (3009712)

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

Risk Level: Medium

CVE: CVE-2014-6319, CVE-2014-6325, CVE-2014-6326, CVE-2014-6336

Description

Multiple vulnerabilities are present in some versions of Microsoft Exchange Server.

Observation

Microsoft Exchange is an industry standard server for providing E-Mail, calendar and contacts services.

Multiple vulnerabilities are present in some versions of Microsoft Exchange Server. The flaw lies in multiple components. Successful exploitation could allow an attacker to obtain sensitive information or elevate its privileges. The Exploit requires the user to open a vulnerable website, email or document.

Microsoft has provided MS14-075 to address these issues. The host appears to be missing this patch.

17402 - (MS14-075) Microsoft Exchange Server OWA URL Redirection Spoofing Information Disclosure (3009712)

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

Risk Level: Medium

CVE: CVE-2014-6336

Description

A vulnerability in some versions of Microsoft Exchange Server could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Exchange Server could lead to privilege escalation.

The flaw lies in the handling of redirection tokens by Microsoft Outlook Web Access. Successful exploitation could allow a remote user to gain elevated privileges.

17403 - (MS14-075) Microsoft Exchange Server OWA Cross-Site Scripting II (3009712)

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

Risk Level: Medium

CVE: CVE-2014-6326

Description

A vulnerability in some versions of Microsoft Exchange Server could lead to cross-site scripting.

Observation

A vulnerability in some versions of Microsoft Exchange Server could lead to cross-site scripting.

The flaw lies in the handling of user-input. Successful exploitation could allow a remote attacker to inject arbitrary web script or HTML code.

17404 - (MS14-075) Microsoft Exchange Server OWA Cross-Site Scripting I (3009712)

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

Risk Level: Medium

CVE: CVE-2014-6325

Description

A vulnerability in some versions of Microsoft Exchange Server could lead to cross-site scripting.

Observation

A vulnerability in some versions of Microsoft Exchange Server could lead to cross-site scripting.

The flaw lies in the handling of user-input. Successful exploitation could allow a remote attacker to inject arbitrary web script or HTML code.

17405 - (MS14-075) Microsoft Exchange Server OWA Token Spoofing Information Disclosure (3009712)

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

Risk Level: Medium

CVE: CVE-2014-6319

Description

A vulnerability in some versions of Microsoft Exchange Server could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Exchange Server could lead to privilege escalation.

The flaw lies in the handling of a request token by Microsoft Outlook Web Access. Successful exploitation could allow a remote user to gain elevated privileges.

17481 - (MS14-085) Vulnerability in Microsoft Graphics Component Could Allow Information (3013126)

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

Risk Level: Medium

CVE: CVE-2014-6355

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 flaw lies in the the Microsoft Graphics component. Successful exploitation could allow an attacker to access potentially sensitive information.

Microsoft has provided MS14-085 to address this issue. The host appears to be missing this patch.

17490 - (MS14-083) Microsoft Excel Global Free Remote Code Execution (3017347)

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

Risk Level: Medium

CVE: CVE-2014-6360

Description

A vulnerability in some versions of Microsoft Excel could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Excel could lead to remote code execution.

The flaw lies in the handling of specially crafted Office files. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17491 - (MS14-083) Microsoft Excel Excel Invalid Pointer Remote Code Execution (3017347)

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

Risk Level: Medium

CVE: CVE-2014-6361

Description

A vulnerability in some versions of Microsoft Excel could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Excel could lead to remote code execution.

The flaw lies in the handling of specially crafted Office files. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17492 - (MS14-085) Microsoft Graphics ASLR Bypass Information Disclosure (3013126)

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

Risk Level: Medium

CVE: CVE-2014-6355

Description

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.

The flaw lies in the handling of JPEG images in memory by the Microsoft Graphics Component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

17494 - (MS14-082) Microsoft Office Component Use-After-Free Remote Code Execution (3017349)

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

Risk Level: Medium

CVE: CVE-2014-6364

Description

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

Observation

A vulnerability in some versions of Microsoft Office could lead to remote code execution.

The flaw lies in the handling of specially crafted Office files. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

17497 - (MS14-080) Microsoft Internet Explorer ASLR Security Bypass (3008923)

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

Risk Level: Medium

CVE: CVE-2014-6368

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to a security bypass.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to a security bypass.

The flaw lies in the ASLR component. Successful exploitation could allow an attacker to bypass security measures. The exploit requires the user to open a vulnerable website, email or document.

17509 - (MS14-080) Microsoft Internet Explorer XSS Filter I Security Bypass (3008923)

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

Risk Level: Medium

CVE: CVE-2014-6328

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to a security bypass.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to a security bypass.

The flaw lies in the XSS Filter component. Successful exploitation could allow an attacker to bypass security measures. The exploit requires the user to open a vulnerable website, email or document.

17510 - (MS14-080) Microsoft Internet Explorer XSS Filter II Security Bypass (3008923)

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

Risk Level: Medium

CVE: CVE-2014-6365

Description

A vulnerability in some versions of Microsoft Internet Explorer could lead to a security bypass.

Observation

A vulnerability in some versions of Microsoft Internet Explorer could lead to a security bypass.

The flaw lies in the XSS Filter component. Successful exploitation could allow an attacker to bypass security measures. The exploit requires the user to open a vulnerable website, email or document.

17512 - (MS14-080) Cumulative Security Update for Internet Explorer (3008923)

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

Risk Level: Medium

CVE: CVE-2014-6327, CVE-2014-6328, CVE-2014-6329, CVE-2014-6330, CVE-2014-6363, CVE-2014-6365, CVE-2014-6366, CVE-2014-6368, CVE-2014-6369, CVE-2014-6373, CVE-2014-6374, CVE-2014-6375, CVE-2014-6376, CVE-2014-8966

Description

Multiple vulnerabilities are present in some versions of Microsoft Internet Explorer.

Observation

Microsoft Internet Explorer is a popular Internet web browser.

Multiple vulnerabilities are present in some versions of Microsoft Internet Explorer. The flaws are due to several memory corruption vulnerabilities. Successful exploitation could allow an attacker to execute remote code.

Microsoft has provided MS14-080 to address these issues. The host appears to be missing this patch.

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.

16993 - Apple QuickTime mvhd Atom Remote Code Execution

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

Risk Level: High

CVE: CVE-2014-4979

Update Details

Recommendation is updated

17511 - Microsoft Internet Explorer display:run-in Use After Free Remote Code Execution Vulnerability

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

Risk Level: High

CVE: CVE-2014-8967

Update Details

Recommendation is updated

181288 - FreeBSD kde-workspace Privilege Escalation (dafa13a8-6e9b-11e4-8ef7-5453ed2e2b49)

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

Risk Level: High

CVE: CVE-2014-8651

Update Details

Risk is updated

184599 - Ubuntu Linux 12.04 USN-2402-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8651

Update Details

Risk is updated

188503 - Fedora Linux 19 FEDORA-2014-14865 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8651

Update Details

Risk is updated

188506 - Fedora Linux 21 FEDORA-2014-14895 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8651

Update Details

Risk is updated

188509 - Fedora Linux 20 FEDORA-2014-14813 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8651

Update Details

Risk is updated

188548 - Fedora Linux 20 FEDORA-2014-15393 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8990

Update Details

Risk is updated

188549 - Fedora Linux 20 FEDORA-2014-15394 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-1693

Update Details

Risk is updated

188559 - Fedora Linux 19 FEDORA-2014-15373 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-8990

Update Details

Risk is updated

17281 - SSLv3 Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-2014-3566

Update Details

Recommendation is updated

93416 - Mandriva Linux MBS1 MDVSA-2014-225 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4975, CVE-2014-8080, CVE-2014-8090

Update Details

Risk is updated

184624 - Ubuntu Linux 12.04, 14.04, 14.10 USN-2412-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8090

Update Details

Risk is updated

58954 - Debian Linux 7.0 DSA-3029-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3616

Update Details

Risk is updated

170400 - Amazon Linux AMI ALAS-2014-421 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2014-3616

Update Details

Risk is updated

181253 - FreeBSD nginx Inject Commands Into SSL Session Vulnerability (77b784bb-3dc6-11e4-b191-f0def16c5c1b)

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

Risk Level: Medium

CVE: CVE-2014-3616

Update Details

Risk is updated

181294 - FreeBSD kwebkitpart, kde-runtime Insufficient Input Validation (890b6b22-70fa-11e4-91ae-5453ed2e2b49)

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

Risk Level: Medium

CVE: CVE-2014-8600

Update Details

Risk is updated

184562 - Ubuntu Linux 14.04 USN-2351-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3616

Update Details

Risk is updated

184619 - Ubuntu Linux 12.04 USN-2414-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8600

Update Details

Risk is updated

188319 - Fedora Linux 21 FEDORA-2014-11251 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3616

Update Details

Risk is updated

188338 - Fedora Linux 19 FEDORA-2014-11370 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3616

Update Details

Risk is updated

188396 - Fedora Linux 20 FEDORA-2014-11415 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-3616

Update Details

Risk is updated

188528 - Fedora Linux 20 FEDORA-2014-15532 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-8600

Update Details

Risk is updated

70014 - netbios-helpers.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.