



2007-MAY-15

## MCAFFEE 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

#### 5153 - Apple Darwin Streaming Server Multiple Vulnerabilities

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

Check Version: 1.3139

CVE: CVE-2007-0748

##### Description

Apple Darwin Streaming Server contains vulnerabilities that may allow for arbitrary code execution or a denial of service attack.

##### Observation

Apple's Darwin Streaming Server is a server that allows for streamed multi-media.

Apple Darwin Streaming Server contains vulnerabilities that may allow for arbitrary code execution or a denial of service attack. The first vulnerability lies in the is\_command function. The second flaw is due to processing of specially crafted trackID values in a Setup request. Successful exploitation of each would involve sending malicious RTSP requests.

#### 38045 - Apple MacOS X 10.4.9 Update Missing

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

Risk Level: High

Check Version: 1.3073

##### Description

The target system is missing the Apple MacOS X 10.4.9 operating system update.

### Observation

Apple MacOS X is an industry standard operating system. The target system is missing the Apple MacOS X 10.4.9 operating system update. This update includes fixes for a number of security issues.

## **38037 - Apple QuickTime .mov JVTCompEncodeFrame Vulnerability**

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

Risk Level: High

Check Version: 1.3077

CVE: CVE-2007-2295

### Description

A vulnerability exists in Apple QuickTime that may allow for remote code execution.

### Observation

QuickTime is a movie player that runs on the Windows and Mac OS X platforms. It is developed by Apple Computers.

A vulnerability is present in Apple QuickTime that may allow for remote code execution. The flaw lies in the JVTCompEncodeFrame function which incorrectly parses malformed .mov files resulting in a segmentation fault. Successful exploitation would involve a victim being coerced to open a malicious .mov file.

## **38038 - Apple QuickTime .mp4 FlipFileTypeAtom\_BtoN Vulnerability**

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

Risk Level: High

Check Version: 1.3077

CVE: CVE-2007-2296

### Description

A vulnerability exists in Apple QuickTime that may allow for remote code execution.

### Observation

QuickTime is a movie player that runs on the Windows and Mac OS X platforms. It is developed by Apple Computers.

A vulnerability is present in Apple QuickTime that may allow for remote code execution. The flaw lies in the FlipFileTypeAtom\_BtoN function which incorrectly parses malformed .MP4 files resulting in a segmentation fault. Successful exploitation would involve a victim being coerced to open a malicious .MP4 file.

### 3553 - McAfee VirusScan Real-Time Detection Enabled

Category: Windows Host Assessment -> Anti-Virus Software  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

Check Version: 1.153

#### Description

McAfee VirusScan On-Access Scanning was not detected as running on the host.

#### Observation

McAfee VirusScan's On-Access Scanning was not running at the time of the scan.

### 5145 - McAfee SecurityCenter Subscription Manager ActiveX Control Buffer Overflow

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

Risk Level: High

Check Version: 1.3168

CVE: CVE-2007-2584

#### Description

A vulnerability in McAfee SecurityCenter Subscription Manager which is present in several McAfee consumer products may allow for remote code execution. The user of vulnerable products would have to visit a malicious Web site for an attack to succeed.

#### Observation

McAfee SecurityCenter provides a user interface to manage McAfee consumer products.

A vulnerability in McAfee SecurityCenter Subscription Manager which is present in several McAfee consumer products may allow for remote code execution. The flaw is found in an ActiveX control that is part of SecurityCenter. The user of vulnerable products would have to visit a malicious Web site for an attack to succeed.

## 5117 - Adobe Photoshop PNG Buffer Overflow Vulnerability

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

Risk Level: High

Check Version: 1.3077

CVE: CVE-2007-2365

### Description

A buffer overflow vulnerability in Adobe Photoshop may allow for remote code execution.

### Observation

Adobe Photoshop is a popular design tool.

A buffer overflow vulnerability in Adobe Photoshop may allow for remote code execution. An attacker might exploit the vulnerability by tricking their victims into opening a maliciously crafted PNG file in Photoshop.

## 5118 - AOL Nullsoft WinAmp MP4 File Handling vulnerability

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

Risk Level: High

Check Version: 1.3141

CVE: CVE-2007-2498

### Description

A vulnerability in Nullsoft Winamp may allow for remote arbitrary code execution.

### Observation

AOL Nullsoft Winamp is a popular media player.

Nullsoft Winamp contains a vulnerability that may allow for arbitrary code execution on a vulnerable host. The flaw is found in the handling of MP4 files. An attacker would need to convince the victim to open a maliciously crafted MP4 file that is present on their system. The vulnerability cannot be exploited by hosting a malicious MP4 file on a Web site since the Winamp player doesn't open MP4 files from Web sites.

## 38039 - Apple MacOS X Security Update 2005-001 Missing

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

Risk Level: Medium

Check Version: 1.3073

### Description

Target system is missing the Apple MacOS X Security Update 2005-001.

### Observation

Apple MacOS X is an industry standard operating system. The target system is missing the Apple MacOS X Security Update 2005-001. This update includes fixes for a number of security issues.

For more information see:

<http://docs.info.apple.com/article.html?artnum=300770>

## **38044 - Apple MacOS X Security Update 2007-004 Missing**

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

Risk Level: Medium

Check Version: 1.3073

### Description

Target system is missing the Apple MacOS X Security Update 2007-004.

### Observation

Apple MacOS X is an industry standard operating system. The target system is missing the Apple MacOS X Security Update 2007-004. This update includes fixes for a number of security issues.

For more information see:

<http://docs.info.apple.com/article.html?artnum=305391>

## **5116 - Sun Java Web Start System Classes Vulnerability**

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

Risk Level: Medium

Check Version: 1.3170

CVE: CVE-2007-2435

### Description

A vulnerability exists in Java Web Start that may allow for a privilege escalation attack.

### Observation

Sun Java Web Start allows for starting of applications via a web browser.

Sun Java Web Start contains a vulnerability that may allow for a privilege escalation. Although complete details have not been released, it is reported that untrusted java applets may elevate privileges through unintended use of System Classes. Successful exploitation would allow a java applet to grant itself privileges.

## **38040 - Apple MacOS X Security Update 2005-002 Missing**

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

Risk Level: Low

Check Version: 1.3073

### Description

Target system is missing the Apple MacOS X Security Update 2005-002.

### Observation

Apple MacOS X is an industry standard operating system. The target system is missing the Apple MacOS X Security Update 2005-002. This update includes fixes for a number of security issues.

For more information see:

<http://docs.info.apple.com/article.html?artnum=300980>

## **38041 - Apple MacOS X Security Update 2005-003 Missing**

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

Risk Level: Low

Check Version: 1.3073

### Description

Target system is missing the Apple MacOS X Security Update 2005-003.

### Observation

Apple MacOS X is an industry standard operating system. The target system is missing the Apple MacOS X Security Update 2005-003. This update includes fixes for a number of security issues.

For more information see:

<http://docs.info.apple.com/article.html?artnum=301061>

### **38042 - Apple MacOS X Security Update 2005-004 Missing**

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

Risk Level: Low

Check Version: 1.3073

#### Description

Target system is missing the Apple MacOS X Security Update 2005-004.

#### Observation

Apple MacOS X is an industry standard operating system. The target system is missing the Apple MacOS X Security Update 2005-004. This update includes fixes for a number of security issues.

For more information see:

<http://docs.info.apple.com/article.html?artnum=301326>

### **5159 - McAfee ePolicy Orchestrator Agent Last Update**

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Informational

Check Version: 1.3151

#### Description

A McAfee ePolicy Orchestrator agent was detected, and the last date of update was found.

#### Observation

McAfee ePolicy Orchestrator is an industry standard central security management hub. It helps keep protection up to date; configure and enforce protection policies; and monitor security status.

### **5158 - McAfee HIPS Enabled And Version Information**

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

Risk Level: Informational

Check Version: 1.3155

#### Description

McAfee Host Intrusion Prevention is installed and enabled.

#### Observation

McAfee Host Intrusion Prevention is an industry standard security application that monitors and blocks unwanted activity and makes it easier to keep desktops safe with multiple proven methods system firewall, signature analysis, and behavioral analysis.

### **5141 - Symbol WAP AP-5131 FTP service detection**

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Informational

Check Version: 1.3119

#### Description

Symbol Wireless Access Point AP-5131 detected.

#### Observation

The remote target is a Symbol AP-5131, FTP server is enabled on port 21.

### **5140 - Symbol WAP AP-5131 HTTP interface detection**

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Informational

Check Version: 1.3119

#### Description

Symbol Wireless Access Point AP-5131 detected.

#### Observation

The remote target is a Symbol AP-5131 wireless access point, HTTP/HTTPS service is enabled on port 80/443.

### **5144 - Symbol Wireless Access Point SP-5131 SNMP use default private community**

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Informational

Check Version: 1.3119

### Description

Symbol Wireless Access Point AP-5131 default community "private" detected.

### Observation

The remote target is a Symbol WAP AP-5131, SNMP server is enabled and use default "public"/"private" community.

## 5143 - Symbol AP-5131 snmp service detected

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Informational

Check Version: 1.3119

### Description

Symbol Wireless Access Point AP-5131 detected.

### Observation

The remote target is a Symbol AP-5131, snmp service is listen on udp port 161, the community is "public".

## 5142 - Symbol WAP AP-5131 Telnet service detected

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Informational

Check Version: 1.3169

### Description

Symbol Wireless Access Point AP-5131 detected.

### Observation

The remote target is a Symbol WAP AP-5131, telnet server is enabled on port 23.

## 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.

## **4451 - (MS06-037) Microsoft Excel Malformed OBJECT record Vulnerability (917285)**

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

Risk Level: High

Check Version: 1.966

CVE: CVE-2006-1306

DISA IAVA: 2006-A-0028

Microsoft ID: MS06-037

## **5062 - (MS07-022) Microsoft Local Kernel EOP Vulnerability (931784)**

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

Risk Level: High

Check Version: 1.3158

CVE: CVE-2007-1206

Microsoft ID: MS07-022

## **5054 - CA BrightStor ARCserve Backup Tape Engine/Portmapper Vulnerabilities**

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

Check Version: 1.3135

CVE: CVE-2006-6076

DISA IAVA: 2007-T-0011

BID: 21221

## **4984 - FactoSystem Weblog Multiple SQL Injection Vulnerabilities**

Category: General Vulnerability Assessment -> NonIntrusive -> Web

Risk Level: Medium

Check Version: 1.2542

CVE: CVE-2002-1499

BID: 5600

## **70014 - netbios-helpers.fasl3.inc**

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

Check Version: 1.3142

### **45000 - ShellLogon.fasl3**

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category

Risk Level: Informational

Check Version: 1.3146

## **DELETED CHECKS**

### **42222 - HP-UX 11.X PHCO\_33142**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42228 - HP-UX 11.X PHCO\_34275**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42229 - HP-UX 11.X PHCO\_34509**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42289 - HP-UX 11.X PHCO\_34764**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42236 - HP-UX 11.X PHKL\_34122**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

#### **42055 - HP-UX 11.X PHNE\_31965**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

#### **42057 - HP-UX 11.X PHNE\_33395**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

#### **42247 - HP-UX 11.X PHNE\_34672**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

#### **42297 - HP-UX 11.X PHNE\_34689**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

#### **42061 - HP-UX 11.X PHNE\_34900**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

#### **42249 - HP-UX 11.X PHNE\_34936**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42250 - HP-UX 11.X PHNE\_34938**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42103 - HP-UX 11.X PHSS\_32260**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42305 - HP-UX 11.X PHSS\_33321**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42307 - HP-UX 11.X PHSS\_33587**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42119 - HP-UX 11.X PHSS\_33842**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42122 - HP-UX 11.X PHSS\_34383**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42265 - HP-UX 11.X PHSS\_34759**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42311 - HP-UX 11.X PHSS\_34760**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42127 - HP-UX 11.X PHSS\_34949**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **42130 - HP-UX 11.X PHSS\_35228**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: High

Check Version: 1.1877

### **30012 - 119985-02 update is not installed**

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

Risk Level: Medium

Check Version: 1.546

### **31503 - 121317-02 update is not installed**

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

Risk Level: Low

### **42286 - HP-UX 11.X PHCO\_32149**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: Informational

Check Version: 1.1877

### **42226 - HP-UX 11.X PHCO\_34214**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: Informational

Check Version: 1.1877

#### **42288 - HP-UX 11.X PHCO\_34215**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: Informational

Check Version: 1.1877

#### **42227 - HP-UX 11.X PHCO\_34240**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: Informational

Check Version: 1.1877

#### **42036 - HP-UX 11.X PHKL\_33268**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: Informational

Check Version: 1.1877

#### **42259 - HP-UX 11.X PHSS\_32732**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: Informational

Check Version: 1.1877

#### **42304 - HP-UX 11.X PHSS\_32741**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: Informational

Check Version: 1.1877

#### **42260 - HP-UX 11.X PHSS\_32976**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: Informational

Check Version: 1.1877

### **42261 - HP-UX 11.X PHSS\_33130**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: Informational

Check Version: 1.1877

### **42262 - HP-UX 11.X PHSS\_33949**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: Informational

Check Version: 1.1877

### **42315 - HP-UX 11.X PHSS\_35435**

Category: SSH Module -> NonIntrusive -> HP/UX Patches and Hotfixes

Risk Level: Informational

Check Version: 1.1877

### **30005 - 118822-30 update is not installed**

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

Risk Level: Informational

Check Version: 1.546

### **30017 - 120467-05 update is not installed**

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

Risk Level: Informational

Check Version: 1.546

### **31464 - 121236-02 update is not installed**

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

Risk Level: Informational

Check Version: 1.1997

### **31466 - 122856-03 update is not installed**

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

Risk Level: Informational

Check Version: 1.1895

### **31471 - 123304-02 update is not installed**

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

Risk Level: Informational

Check Version: 1.1895

### **31473 - 124206-02 update is not installed**

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

Risk Level: Informational

Check Version: 1.1895

### **30791 - 118844-30 update is not installed**

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

Risk Level: Informational

### **30801 - 120468-05 update is not installed**

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

Risk Level: Informational

### **31491 - 122857-04 update is not installed**

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

Risk Level: Informational

Check Version: 1.1895

### **31495 - 124207-02 update is not installed**

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

Risk Level: Informational

Check Version: 1.1895

### **30060 - 113319-25 update is not installed**

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

Risk Level: Informational

Check Version: 1.2830

### **31479 - 121316-02 update is not installed**

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

Risk Level: Informational

### **30818 - 113719-19 update is not installed**

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

Risk Level: Informational

Check Version: 1.2830

### **30821 - 113924-02 update is not installed**

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

Risk Level: Informational

## **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**

PrimeSupport ServicePortal: <https://mysupport.nai.com/login.asp>

Multi-National Phone Support available here:

<http://www.mcafeesecurity.com/us/contact/home.htm>

PGP Key: <http://www.foundstone.com/pgpkeys/techsupport.asc>

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2004-2007 McAfee, Inc.

McAfee is a registered trademark of McAfee, Inc. and/or its affiliates