



2006-OCT-30

## 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

#### 4718 - Oracle Releases October 2006 Oracle Critical Patch Update

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

Check Version: 1.1619

CVE: CVE-2006-5377

DISA IAVA: 2006-A-0047

#### Description

Multiple vulnerabilities have been addressed by Oracle in the Critical Patch Update for October 2006.

#### Observation

Oracle is a popular database application.

Vulnerabilities exist in Oracle Database applications that may at worst allow for complete system compromise. Many of these vulnerabilities allow for remote exploitation without authentication. Oracle has released the Critical Update for October 2006 to address these. The affected components include:

- Oracle Pharmaceutical Applications
- Oracle PeopleSoft Enterprise Tools
- Oracle PeopleSoft Enterprise Portal
- Oracle PeopleSoft Enterprise PeopleTools
- Oracle Oracle9i Standard Edition
- Oracle Oracle9i Personal Edition
- Oracle Oracle9i Enterprise Edition
- Oracle Oracle9i Application Server

Oracle Oracle8i Standard Edition  
Oracle Oracle8i Enterprise Edition  
Oracle Oracle10g Standard Edition  
Oracle Oracle10g Personal Edition  
Oracle Oracle10g Enterprise Edition  
Oracle Oracle10g Application Server  
Oracle OneWorld Tools SP23  
Oracle JD Edwards EnterpriseOne  
Oracle HTML DB  
Oracle E-Business Suite  
Oracle Developer Suite  
Oracle Collaboration Suite Release  
Oracle Application Server

## 4696 - (MS05-012) Microsoft Windows COM Structured Storage

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

Risk Level: High

Check Version: 1.1564

CVE: CAN-2005-0047

DISA IAVA: 2005-A-0007

ARMY IAVA: 2005-A-0007

Microsoft ID: MS05-012

Microsoft KB: 873333

SANS: Yes

### Description

A remote code execution vulnerability exists in the Microsoft OLE functionality included with Windows operating system.

### Observation

Microsoft Windows is an industry standard operating system. Windows includes Object Linking and Embedding (OLE) functionality that helps software combine components to create more complex components.

A critical vulnerability is present in OLE that may allow for an attacker to take complete control of an affected system. An attacker could exploit this vulnerability by crafting a malicious document and tricking a user into opening it.

Affected Systems:

Microsoft Windows NT 4.0  
Microsoft Windows 2000  
Microsoft Windows XP SP0, SP1, SP2  
Microsoft Windows Server 2003

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-012.msp>

## 4697 - (MS05-025) Microsoft Internet Explorer PNG Rendering Memory Corruption

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

Risk Level: High

CVE: CAN-2005-1211

DISA IAVA: 2005-A-0016

Microsoft ID: MS05-025

Microsoft KB: KB883939

SANS: Yes

### Description

A cumulative update for Microsoft Internet Explorer is not installed.

### Observation

Microsoft Internet Explorer (IE) is an industry standard web browser.

A remote code execution vulnerability is present in code included with IE that is responsible for rendering PNG encoded images. This vulnerability can be exploited by viewing malicious images with IE. This issue is also exploitable via e-mail.

Affected software:

Microsoft Internet Explorer 5.5 SP3

Microsoft Internet Explorer 5.5 SP4

Microsoft Internet Explorer 6.0 SP1

Microsoft Internet Explorer 6.0 for Microsoft Windows XP Service Pack 2

Microsoft Internet Explorer 6.0 for Microsoft Windows Server 2003

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-025.mspx>

## 4705 - (MS05-053) Microsoft Windows Graphics Rendering Engine Overflow

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

Risk Level: High

CVE: CAN-2005-2123

DISA IAVA: 2005-A-0039

Microsoft ID: MS05-053

Microsoft KB: KB896424

SANS: Yes

### Description

A buffer overflow vulnerability is present in the Microsoft Windows Graphics Rendering Engine.

### Observation

Microsoft Windows is an industry standard operating system. Windows includes support for advanced graphics rendering.

A vulnerability is present in the Windows Graphics Rendering Engine allowing attackers to control any program that renders Windows Metafile (WMF) and Enhanced Metafile (EMF) images.

Affected systems:

Microsoft Windows Server 2003 Service Pack 1  
Microsoft Windows Server 2003 Service Pack 0  
Microsoft Windows XP Service Pack 2  
Microsoft Windows XP Service Pack 1  
Microsoft Windows 2000 Service Pack 4

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-053.msp>

## **4706 - (MS05-053) Microsoft Windows Windows Metafile WMF Overflow**

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

Risk Level: High

CVE: CAN-2005-2124

DISA IAVA: 2005-A-0039

Microsoft ID: MS05-053

Microsoft KB: KB896424

SANS: Yes

### Description

A buffer overflow vulnerability is present in the Microsoft Windows Graphics Rendering Engine.

### Observation

Microsoft Windows is an industry standard operating system. Windows includes support for advanced graphics rendering.

A vulnerability is present in the rendering of Windows Metafile (WMF) image format allowing attackers to control any program that renders WMF images.

Affected systems:

Microsoft Windows Server 2003 Service Pack 1  
Microsoft Windows Server 2003 Service Pack 0  
Microsoft Windows XP Service Pack 2  
Microsoft Windows XP Service Pack 1  
Microsoft Windows 2000 Service Pack 4

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-053.msp>

## **4698 - (MS05-038) Microsoft Internet Explorer Web Folder Behaviors Cross-Domain**

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

Risk Level: High

CVE: CAN-2005-1989

DISA IAVA: 2005-A-0024

ARMY IAVA: 2005-A-0024

Microsoft ID: MS05-038

Microsoft KB: KB896727

SANS: Yes

### Description

Microsoft Internet Explorer is missing a cumulative update.

### Observation

Microsoft Internet Explorer is an industry standard web browser.

A vulnerability is present in Internet Explorer in how URLs are handled when browsing from a web page to a web folder. It may be possible to exploit this vulnerability to gain information about a target system, or even to trick a user into executing malicious code.

CVE:  
CAN-2005-1989

Affected software:

Microsoft Internet Explorer 6.0 for Windows Server 2003 Service Pack 0  
Microsoft Internet Explorer 6.0 for Windows Server 2003 Service Pack 1  
Microsoft Internet Explorer 6.0 for Windows XP Service Pack 2  
Microsoft Internet Explorer 6.0 SP1  
Microsoft Internet Explorer 5.0

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-038.mspx>

## **4699 - (MS05-038) Microsoft Internet Explorer COM Instantiation Memory Corruption**

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

Risk Level: High

CVE: CAN-2005-1990

DISA IAVA: 2005-A-0024

ARMY IAVA: 2005-A-0024

Microsoft ID: MS05-038

Microsoft KB: KB896727

SANS: Yes

### Description

Microsoft Internet Explorer is missing a cumulative update.

### Observation

Microsoft Internet Explorer is an industry standard web browser.

A memory corruption vulnerability is present in code that handles ActiveX control instantiation. If IE attempts to instantiate a COM object in the same manner as an ActiveX control, memory may be corrupted and arbitrary code execution may be possible.

CVE:  
CAN-2005-1990

Affected software:

Microsoft Internet Explorer 6.0 for Windows Server 2003 Service Pack 0  
Microsoft Internet Explorer 6.0 for Windows Server 2003 Service Pack 1  
Microsoft Internet Explorer 6.0 for Windows XP Service Pack 2  
Microsoft Internet Explorer 6.0 SP1  
Microsoft Internet Explorer 5.0

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-038.mspx>

## **4702 - (MS05-051) Microsoft Windows MSDTC Denial of Service**

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

Risk Level: High

CVE: CAN-2005-1979

DISA IAVA: 2005-A-0030

Microsoft ID: MS05-051

Microsoft KB: KB902400

SANS: Yes

### Description

Microsoft Windows contains a denial of service in the Microsoft Distributed Transaction Coordinator (MSDTC) service.

### Observation

MSDTC allows you to coordinate transactions between multiple SQL and web servers.

The MSDTC service contains a denial of service allowing remote attackers to stop the service from responding.

Affected systems:

Microsoft Windows Server 2003 Service Pack 1  
Microsoft Windows Server 2003 Service Pack 0  
Microsoft Windows XP Service Pack 2  
Microsoft Windows XP Service Pack 1  
Microsoft Windows 2000 Service Pack 4

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-051.msp>

## **4703 - (MS05-051) Microsoft Windows MSDTC Distributed Denial of Service**

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

Risk Level: High

CVE: CAN-2005-1980

DISA IAVA: 2005-A-0030

Microsoft ID: MS05-051

Microsoft KB: KB902400

SANS: Yes

### Description

Microsoft Windows contains a denial of service in the Microsoft Distributed Transaction Coordinator (MSDTC) service.

### Observation

MSDTC allows you to coordinate transactions between multiple SQL and web servers.

The MSDTC service contains a denial of service allowing remote attackers to stop the service from responding. In addition a specifically crafted message could be transferred through the affected system to another TIP server causing further systems to be affected.

Affected systems:

Microsoft Windows Server 2003 Service Pack 1  
Microsoft Windows Server 2003 Service Pack 0  
Microsoft Windows XP Service Pack 2  
Microsoft Windows XP Service Pack 1  
Microsoft Windows 2000 Service Pack 4

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-051.msp>

## 4704 - (MS05-051) Microsoft Windows MSDTC Overflow

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

Risk Level: High

CVE: CAN-2005-2119

DISA IAVA: 2005-A-0030

Microsoft ID: MS05-051

Microsoft KB: KB902400

SANS: Yes

### Description

Microsoft Windows contains a buffer overflow in the Microsoft Distributed Transaction Coordinator (MSDTC) service.

### Observation

MSDTC allows you to coordinate transactions between multiple SQL and web servers.

The MSDTC service contains a buffer overflow allowing remote attackers to execute code.

Affected systems:

Microsoft Windows Server 2003 Service Pack 1

Microsoft Windows Server 2003 Service Pack 0

Microsoft Windows XP Service Pack 2

Microsoft Windows XP Service Pack 1

Microsoft Windows 2000 Service Pack 4

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-051.msp>

## 4695 - (MS05-002) Microsoft Windows Kernel Denial of Service

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

Risk Level: High

CVE: CAN-2004-1305

DISA IAVA: 2005-A-0001

ARMY IAVA: 2005-A-0001

Microsoft ID: MS05-002

Microsoft KB: 891711

SANS: Yes

### Description

A denial of service exists in the way cursor and icon formats are handled in Microsoft Windows.

### Observation

A vulnerability exists in the way that cursor, animated cursor, and icon formats are handled allowing attackers to create a malicious cursor or icon file resulting in a denial of service.

CVE:  
CAN-2004-1305

Affected Systems:

Microsoft Windows NT 4.0 Server SP6a  
Microsoft Windows 2000 SP3, SP4  
Microsoft Windows XP SP1  
Microsoft Windows Server 2003

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-002.msp>

## **4700 - (MS05-049) Microsoft Windows Ink Filename Shell Handling**

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

Risk Level: Medium

CVE: CAN-2005-2118

DISA IAVA: 2005-A-0027

Microsoft ID: MS05-049

Microsoft KB: KB900725

SANS: Yes

### Description

Microsoft Windows contains a remote code execution vulnerability in the shell component.

### Observation

Microsoft Windows is an industry standard operating system.

A remote code execution vulnerability is present when processing filenames with a .lnk file name extension.

Affected systems:

Microsoft Windows Server 2003 Service Pack 1  
Microsoft Windows Server 2003 Service Pack 0  
Microsoft Windows XP Service Pack 2  
Microsoft Windows XP Service Pack 1  
Microsoft Windows 2000 Service Pack 4

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-049.mspx>

## 4701 - (MS05-049) Microsoft Windows Web View Script Injection

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

Risk Level: Medium

CVE: CAN-2005-2122

DISA IAVA: 2005-A-0027

Microsoft ID: MS05-049

SANS: Yes

### Description

Microsoft Windows contains a remote code execution vulnerability in the shell component.

### Observation

Microsoft Windows is an industry standard operating system.

A remote code execution vulnerability is present in the Windows Explorer Web View when it handles certain HTML characters in preview fields.

Affected systems:

Microsoft Windows Server 2003 Service Pack 1  
Microsoft Windows Server 2003 Service Pack 0  
Microsoft Windows XP Service Pack 2  
Microsoft Windows XP Service Pack 1  
Microsoft Windows 2000 Service Pack 4

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-049.msp>

## **4707 - (MS05-054) Microsoft Internet Explorer Download Dialog Box Manipulation**

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

Risk Level: Medium

CVE: CAN-2005-2829

DISA IAVA: 2005-A-0045

Microsoft ID: MS05-054

Microsoft KB: KB905915

### Description

A cumulative security patch for Microsoft Internet Explorer has not been installed on the host.

### Observation

Microsoft Windows is an industry standard operating system. Windows includes the Internet Explorer (IE) web browser.

Internet Explorer contains a potential remote code vulnerability due to the way it displays file download dialog boxes and accepts user input during interaction with a Web page.

Affected systems:

Microsoft Windows Server 2003 SP0

Microsoft Windows Server 2003 SP1

Microsoft Windows Server 2003 R2

Microsoft Windows XP SP1

Microsoft Windows XP SP2

Microsoft Windows 2000 SP4 + IE 5.01

Microsoft Windows 2000 SP4 + IE 6.0 SP1

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-054.msp>

## **4708 - (MS05-054) Microsoft Internet Explorer HTTPS Proxy**

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

Risk Level: Medium

CVE: CAN-2005-2830

DISA IAVA: 2005-A-0045

Microsoft ID: MS05-054

Microsoft KB: KB905915

SANS: Yes

### Description

A cumulative security patch for Microsoft Internet Explorer has not been installed on the host.

### Observation

Microsoft Windows is an industry standard operating system. Windows includes the Internet Explorer (IE) web browser.

Internet Explorer contains an information disclosure vulnerability allowing an attacker to read web addresses in clear text sent to a proxy server despite the HTTPS connection.

Affected systems:

Microsoft Windows Server 2003 SP0

Microsoft Windows Server 2003 SP1

Microsoft Windows Server 2003 R2

Microsoft Windows XP SP1

Microsoft Windows XP SP2

Microsoft Windows 2000 SP4 + IE 5.01

Microsoft Windows 2000 SP4 + IE 6.0 SP1

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-054.msp>

## **4709 - (MS05-054) Microsoft Internet Explorer COM Instantiation Memory Corruption**

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

Risk Level: Medium

CVE: CAN-2005-2831

DISA IAVA: 2005-A-0045

Microsoft ID: MS05-054

Microsoft KB: KB905915

### Description

A cumulative security patch for Microsoft Internet Explorer has not been installed on the host.

## Observation

Microsoft Windows is an industry standard operating system. Windows includes the Internet Explorer (IE) web browser.

Internet Explorer contains a remote code execution vulnerability due to the way it incorrectly instantiates COM objects that should not be loaded.

Affected systems:

Microsoft Windows Server 2003 SP0  
Microsoft Windows Server 2003 SP1  
Microsoft Windows Server 2003 R2  
Microsoft Windows XP SP1  
Microsoft Windows XP SP2  
Microsoft Windows 2000 SP4 + IE 5.01  
Microsoft Windows 2000 SP4 + IE 6.0 SP1

For more information see:

<http://www.microsoft.com/technet/security/bulletin/MS05-054.mspx>

## **4715 - Novell eDirectory Stack Overflow Remote Code Execution Vulnerability**

Category: General Vulnerability Assessment -> Intrusive -> Web

Risk Level: Informational

Check Version: 1.1602

## Description

A stack-overflow vulnerability exists in Novell eDirectory that may allow for remote arbitrary-code-execution attacks.

## Observation

Novell's eDirectory is a solution for directory services and user management. Novell's iMonitor is a Web-based management interface for eDirectory.

A stack-overflow vulnerability exists in Novell eDirectory server that may allow for remote arbitrary-code-execution attacks at the level of the server, typically run as admin. The vulnerability is a boundary error in BuildRedirectURL(), part of the HTTP protocol stack httpstk within iMonitor. It can be triggered by sending the function a malicious, specially-crafted host HTTP header that is longer than 64 bytes.

## **4712 - Kerio WinRoute Firewall Remote Denial-of-Service Vulnerability**

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

Risk Level: Informational

Check Version: 1.1592

### Description

Multiple vulnerabilities exist in Kerio WinRoute Firewall that may allow for remote denial-of-service (DoS) attacks.

### Observation

Kerio WinRoute Firewall is a corporate and enterprise gateway firewall solution developed by Kerio.

Two design flaws exist in Kerio WinRoute Firewall that may allow for remote denial-of-service (DoS) attacks. These vulnerabilities are failures to handle exceptions. The first vulnerability could be triggered when WinRoute receives malformed DNS responses. The second vulnerability could be triggered when four or more DNS servers are specified to WinRoute.

WinRoute 6.2.2 and prior versions are affected.

## 4716 - AOL Nullsoft Winamp Lyrics3 Heap Overflow Vulnerability

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

Risk Level: Informational

Check Version: 1.1616

### Description

A heap-overflow vulnerability exists in AOL Nullsoft Winamp that may allow for remote arbitrary-code-execution attacks. A user would have to click on a malicious file URI for an attack to work.

### Observation

AOL Nullsoft Winamp is a media player for Windows operating systems. It is owned by AOL.

A vulnerability exists in AOL Nullsoft Winamp that may allow for remote arbitrary-code-execution attacks. There is a heap overflow in the Lyrics3 parsing code. A user would have to be coerced into clicking a malicious file URI for this buffer overflow to be exploited. Code execution would be at the level of the current user.

## 4717 - AOL Nullsoft Winamp Ultravox Header Heap Overflow Vulnerability

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

Risk Level: Informational

Check Version: 1.1616

### Description

A heap-overflow vulnerability exists in AOL Nullsoft Winamp that may allow for remote arbitrary-code-execution attacks. A user would have to click on a malicious file URI for an attack to work.

### Observation

AOL Nullsoft Winamp is a media player for Windows operating systems. It is owned by AOL.

A vulnerability exists in AOL Nullsoft Winamp that may allow for remote arbitrary-code-execution attacks. A heap overflow in the Ultravox protocol handler is exposed because of an error in the handling of the 'ultravox-max-msg' header. A user would have to be coerced into clicking a malicious file URI for this buffer overflow to be exploited. Code execution would be at the level of the current user.

## 4721 - Microsoft Internet Explorer Popup Address Bar Spoofing Vulnerability

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

Risk Level: Informational

Check Version: 1.1621

### Description

A vulnerability exists in Microsoft Internet Explorer that may allow for phishing attacks.

### Observation

Microsoft Internet Explorer (IE) is an industry-standard Web browser developed by Microsoft.

A vulnerability exists in Microsoft IE that may allow for phishing attacks. Using a specially-crafted URL, it is possible to create an Internet explorer pop-up window with a spoofed address bar. The user may think that this popup is from a trusted site that opens in a normal window.

Successful exploitation would involve a user being coerced into clicking a malicious link. The victim would further need to input sensitive information into the accompanying pop-up window or follow further malicious links from this 'trusted' pop-up.

## 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.

### **1034 - Sendmail Daemon Mode Local Privilege Escalation**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-1999-0130

### **1036 - Sendmail EXPN and VRFY commands Remote Buffer Overflow**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-1999-0203

### **1035 - Sendmail GECOS Local Buffer Overflow**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-1999-0131

### **1601 - Sendmail NOCHAR Address Header Buffer Overflow / DNS Maps Remote Denial-of-Service**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-2003-0161

DISA IAVA: 2003-B-0003

ARMY IAVA: 2003-A-0011, 2003-B-0004

### **1590 - Sendmail Header Processing Buffer Overflow**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-2002-1337

DISA IAVA: 2003-A-0002

ARMY IAVA: 2003-B-0004

### **1913 - Sendmail SMTP HELO Buffer Overflow**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-1999-0098

### **2396 - Sendmail Large Debug Value Buffer Overflow**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-1999-1309

### **2395 - Sendmail Remote MIME Buffer Overflow**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-1999-0047

ARMY IAVA: 1999-X-034

### **2389 - Sendmail 8.12.9 Prescan Buffer Overflow**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-2003-0694

DISA IAVA: 2003-B-0005

ARMY IAVA: 2003-B-0005

### **2393 - Sendmail Pipe Command Execution**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-1999-0163

### **2055 - Sendmail strtok() Prescan Buffer Overflow**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-2003-0694

DISA IAVA: 2003-B-0005

ARMY IAVA: 2003-B-0005

### **2388 - Sendmail Ruleset Parsing Buffer Overflow**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-2003-0681

DISA IAVA: 2003-B-0005

ARMY IAVA: 2004-T-5007

### **2383 - Sendmail Debug Command Allows Command Execution**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-1999-0095

### **1032 - Sendmail 8.8.1 MIME Remote Buffer Overflow**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625

CVE: CVE-1999-0206

### **1033 - Sendmail 8.8.4 MIME overflow**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: High

Check Version: 1.1625  
CVE: CVE-1999-0047  
ARMY IAVA: 1999-X-034

### **3437 - Mozilla Suite DOM Privilege Escalation**

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

Risk Level: High

Check Version: 1.1617

### **3445 - Mozilla Suite Javascript Vulnerabilities**

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

Risk Level: High

Check Version: 1.1617

CVE: CVE-2005-1477

DISA IAVA: 2005-T-0014

ARMY IAVA: 2005-T-0014

SANS: Yes

### **3843 - Mozilla Suite non-DOM Privilege Escalation**

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

Risk Level: High

Check Version: 1.1617

CVE: CVE-2005-1532

DISA IAVA: 2005-T-0014

### **3906 - Mozilla Suite Function Object Traversal Vulnerability**

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

Risk Level: High

Check Version: 1.1617

### **3457 - Mozilla Suite Javascript Security Bypass**

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

Risk Level: High

Check Version: 1.1617

DISA IAVA: 2005-T-0014

### **3465 - Mozilla Suite Favicons Code Execution**

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

Risk Level: High

Check Version: 1.1617

### **3324 - Mozilla Browser Sidebar Panel Remote Code Execution**

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

Risk Level: High

Check Version: 1.1617

### **4572 - Sendmail Multi-Part MIME Message Handling Denial of Service**

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

Check Version: 1.1625

### **2198 - Telnet Daemon is Running**

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

Check Version: 1.1626

CVE: CVE-1999-0619

### **2405 - Sendmail Multiple Connection Denial-of-Service**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

CVE: CVE-1999-0478

### **2404 - Sendmail SunOS /usr/bin Vulnerability**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

CVE: CVE-1999-1506

### **2209 - Sendmail bt Option Negative Index Overflow**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

### **2210 - Sendmail DNS TXT Record Overflow**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

CVE: CVE-2002-0906

### **2400 - Sendmail Dropped Privileges**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

CVE: CVE-2001-0713

### **2399 - Sendmail DNS Remote Denial-of-Service**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

CVE: CVE-2003-0688

### **2192 - Sendmail ETRN Denial-of-Service**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

CVE: CVE-1999-1109

### **2397 - Sendmail Improper Mail From Remote Root Compromise**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

CVE: CVE-1999-0203

### **2208 - Sendmail Local Debug Signedness Vulnerability**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

CVE: CVE-2001-0653

### **2193 - Sendmail maillocal Denial-of-Service**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

CVE: CVE-2000-0319

### **2394 - Sendmail Newline Remote Denial-of-Service**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

CVE: CVE-2000-0319

### **2390 - Sendmail WIZ Command Allows Root Access**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

CVE: CVE-1999-0145

### **2382 - Sendmail Vulnerable Group Permissions**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

CVE: CVE-1999-0129

### **2381 - Sendmail and Vacation Program Code Execution**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Medium

Check Version: 1.1625

CVE: CVE-1999-0057

### **3929 - Mozilla Suite Chrome Window Spoofing**

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

Risk Level: Medium

Check Version: 1.1617

### **3902 - Mozilla Suite Content Generated Event Vulnerability**

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

Risk Level: Medium

Check Version: 1.1617

### **2818 - Mozilla Browser Cookie Directory Traversal**

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

Risk Level: Medium

Check Version: 1.1617

CVE: CVE-2003-0594

### **2815 - Mozilla Browser Frame Injection**

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

Risk Level: Medium

Check Version: 1.1617

CVE: CVE-2004-0718

### **3833 - Mozilla Suite Frame Spoof Vulnerability**

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

Risk Level: Medium

Check Version: 1.1617

CVE: CVE-2005-1937

SANS: Yes

### **3923 - Mozilla Suite XMLHttpRequest Header Spoof**

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

Risk Level: Medium

Check Version: 1.1617

### **3460 - Mozilla Suite Install Object Vulnerability**

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

Risk Level: Medium

Check Version: 1.1617

### **3788 - Mozilla Suite InstallTrigger Vulnerability**

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

Risk Level: Medium

Check Version: 1.1617

CVE: CVE-2005-2263

### **3830 - Mozilla Suite InstallVersion.compareTo Vulnerability**

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

Risk Level: Medium

Check Version: 1.1617

CVE: CVE-2005-2265

### **3838 - Mozilla Suite Javascript Prompt Spoof**

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

Risk Level: Medium

Check Version: 1.1617

CVE: CVE-2005-2268

SANS: Yes

### **3462 - Mozilla Suite Popup Vulnerability**

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

Risk Level: Medium

Check Version: 1.1617

### **2813 - Mozilla Browser "shell:" Handler**

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

Risk Level: Medium

Check Version: 1.1617

CVE: CVE-2004-0648

### **2817 - Mozilla Browser Address Bar Spoofing**

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

Risk Level: Medium

Check Version: 1.1617

### **3835 - Mozilla Suite top.focus() Vulnerability**

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

Risk Level: Medium

Check Version: 1.1617

CVE: CVE-2005-2266

### **3899 - Mozilla Suite XBL Script Vulnerability**

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

Risk Level: Medium

Check Version: 1.1617

### **3920 - Mozilla Suite XBM Heap Overflow**

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

Risk Level: Medium

Check Version: 1.1617

### **3904 - Mozilla Suite XHTML Node Spoofing**

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

Risk Level: Medium

Check Version: 1.1617

### **2814 - Mozilla Browser XPInstall Dialog Box**

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

Risk Level: Medium

Check Version: 1.1617

CVE: CVE-2004-0762

### **2819 - Mozilla Browser Zombie Document Cross-Site Scripting**

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

Risk Level: Medium

Check Version: 1.1617

CVE: CVE-2004-0191

### **3323 - Mozilla Browser GIF Heap Overflow**

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

Risk Level: Medium

Check Version: 1.1617

### **3325 - Mozilla Drag and Drop Loading of Privileged XUL**

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

Risk Level: Medium

Check Version: 1.1617

### **2401 - Sendmail Decode Aliases**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Low

Check Version: 1.1625

CVE: CVE-1999-0096

### **2398 - Sendmail Hop Count Remote Denial-of-Service**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Low

Check Version: 1.1625

CVE: CVE-2001-0714

### **2216 - Sendmail Local Debug Mode Information Leak**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Low

Check Version: 1.1625

CVE: CVE-2001-0715

### **2386 - Sendmail Signal Handling Race Condition**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Low

Check Version: 1.1625

CVE: CVE-2001-1349

### **2385 - Sendmail SMRSH Bypass**

Category: General Vulnerability Assessment -> NonIntrusive -> UNIX

Risk Level: Low

Check Version: 1.1625

CVE: CVE-2002-1165

### **3927 - Mozilla Suite About: Vulnerability**

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

Risk Level: Low

Check Version: 1.1617

### **3439 - Mozilla Suite Global Scope Pollution**

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

Risk Level: Low

Check Version: 1.1617

### **3432 - Mozilla Suite Search Plugin Vulnerability**

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

Risk Level: Low

Check Version: 1.1617

### **3351 - Mozilla Suite Information Disclosure**

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

Risk Level: Low

Check Version: 1.1617

### **70002 - http-helpers.fasl3.inc**

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

Risk Level: Informational

Check Version: 1.1586

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

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

Risk Level: Informational

Check Version: 1.1621

### 2837 - All Drives NTFS Policy

Category: Windows Host Assessment -> Security Policy/Options  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

Check Version: 1.1594

### 4029 - Default TsInternetUser Account Has Not Been Renamed

Category: Windows Host Assessment -> Security Policy/Options  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Informational

Check Version: 1.1626

## DELETED CHECKS

### 4286 - Sun Solaris lpd transfer job Buffer Overflow

Category: General Vulnerability Assessment -> Intrusive -> UNIX

Risk Level: High

Check Version: 1.340

CVE: CVE-2001-0353

### 4626 - Administrator Account Has No Password Lookup by SID

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

Risk Level: High

Check Version: 1.1397

CVE: CVE-1999-0504

DISA IAVA: 2003-A-0002

## 4627 - Guest Account Has No Password Lookup by SID

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

Risk Level: Medium

Check Version: 1.1397

CVE: CVE-1999-0504

DISA IAVA: 2003-A-0002

## 4628 - User Accounts Have Blank Password

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

Risk Level: Medium

Check Version: 1.1397

## 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.

## MCAFFEE 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.