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

22040 - Oracle WebLogic Server Critical Patch Update April 2017

Category: Windows Host Assessment -> Miscellaneous
(Category REQUIRES CREDENTIALS)
Risk Level: High

Description
Multiple vulnerabilities are present in some versions of Oracle WebLogic Server.

Observation
Oracle WebLogic Server is a Java EE application server.

Multiple vulnerabilities are present in some versions of Oracle WebLogic Server. The flaws lie in several components. Successful exploitation could allow an attacker to retrieve sensitive data, cause a denial of service condition or remotely execute arbitrary code on the target system.


Category: Windows Host Assessment -> Patches and Hotfixes
(Category REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8588

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

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

The flaw exists in the way that Microsoft WordPad parses specially crafted files. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

22121 - (APSB17-21) Vulnerabilities In Adobe Flash Player

Category: Windows Host Assessment -> Adobe Patches Only
(Category REQUIRES CREDENTIALS)
Risk Level: High

Description
Multiple vulnerabilities are present in some versions of Adobe Flash Player.
Adobe Flash Player is a software for viewing rich Internet applications, streaming audio, video and multimedia files. Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws are due to several memory issues. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system or disclose private information.

The update provided by Adobe bulletin APSB17-21 resolves these issues. The target system is missing this update.

22122 - (APSB17-21) Vulnerabilities In Adobe Flash Player
Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: High

Description
Multiple vulnerabilities are present in some versions of Adobe Flash Player.

Internet Explorer is an Internet browser developed by Microsoft.
A memory corruption vulnerability is present in some versions of Microsoft Internet Explorer. The flaw is due to improper handling of objects in memory. Successful exploitation could allow a remote attacker to execute arbitrary code in the context of the current user.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8606

Description
A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer and Edge.

Observation
Internet Explorer and Edge are Internet browsers developed by Microsoft.

A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer and Edge. The flaw is due to improper handling of objects in memory. Successful exploitation could allow a remote attacker to execute arbitrary code in the context of the current user.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8607

Description
A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer and Edge.

Observation
Internet Explorer and Edge are Internet browsers developed by Microsoft.

A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer and Edge. The flaw is due to improper handling of objects in memory. Successful exploitation could allow a remote attacker to execute arbitrary code in the context of the current user.

22059 - (MSPT-Jul2017) Microsoft Scripting Engine Memory Corruption Vulnerability (CVE-2017-8608)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8608

Description
A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer and Edge.

Observation
Internet Explorer and Edge are Internet browsers developed by Microsoft.

A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer and Edge. The flaw is due to improper handling of objects in memory. Successful exploitation could allow a remote attacker to execute arbitrary code in the context of the current user.

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8609

Description
A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer.

Observation
Internet Explorer is an Internet browser developed by Microsoft.

A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer. The flaw is due to improper handling of objects in memory. Successful exploitation could allow a remote attacker to execute arbitrary code in the context of the current user.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8618

Description
A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer.

Observation
Internet Explorer is an Internet browser developed by Microsoft.

A remote code execution vulnerability is present in some versions of Microsoft Internet Explorer. The flaw is due to improper handling of objects in memory. Successful exploitation could allow a remote attacker to execute arbitrary code in the context of the current user.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8595

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

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

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email, or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8596

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

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

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email, or document.

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8598

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

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

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email, or document.

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8601

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

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

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email, or document.

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8603

Description
A vulnerability in some versions of Microsoft Edge could lead to remote code execution.
Observation
A vulnerability in some versions of Microsoft Edge could lead to remote code execution.

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email, or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8604

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

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

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email, or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8605

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

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

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email, or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8610

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

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

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email, or document.
code. The exploit requires the user to open a vulnerable website, email, or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8617

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

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

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email, or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8619

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

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

The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email, or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2017-8590

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

The flaw exits when the Windows Common Log File System (CLFS) driver improperly handles objects in memory. Successful exploitation could allow a local user to gain elevated privileges.

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

Observation
A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Explorer component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.


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

Observation
A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw lies in the Search component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the attacker to have valid credentials to the vulnerable system.

22117 - Microsoft Windows Azure AD Connect Elevation of Privilege Vulnerability (4033453)

Description
A privilege escalation vulnerability is present in some versions of Microsoft Windows Azure AD Connect.

Observation
Microsoft Windows Azure AD Connect is Microsoft connection software to Azure Active Directory. A privilege escalation vulnerability is present in some versions of Microsoft Windows Azure AD Connect. The flaw is due to writeback being misconfigured during enablement. Successful exploitation could allow an attacker to reset passwords and access on-premises AD privileged user accounts.


Description
An information disclosure vulnerability is present in some versions of Microsoft ASP.NET.

**Observation**

ASP.NET is a server-side web application framework developed by Microsoft.

An information disclosure vulnerability is present in some versions of Microsoft ASP.NET. The flaw is due to improper handling of objects in memory. Successful exploitation could allow a remote attacker to obtain sensitive information.


Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: Medium  
CVE: CVE-2017-8585

**Description**

A denial of service vulnerability is present in some versions of Microsoft .NET Framework.

**Observation**

.NET Framework is a software framework developed by Microsoft.

A denial of service vulnerability is present in some versions of Microsoft .NET Framework. The flaw is due to improper handling of specially crafted web requests. Successful exploitation could allow a remote attacker to cause a denial of service.


Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: Medium  
CVE: CVE-2017-8599

**Description**

A vulnerability in some versions of Microsoft Edge could lead to security bypass.

**Observation**

A vulnerability in some versions of Microsoft Edge could lead to security bypass.

The flaw lies in the Same Origin Policy component. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. The exploit requires the user to open a vulnerable website, email, or document.


Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)  
Risk Level: Medium  
CVE: CVE-2017-8611

**Description**

A vulnerability in some versions of Microsoft Edge could lead to spoofing.

**Observation**

A vulnerability in some versions of Microsoft Edge could lead to spoofing.
The flaw lies in the HTTP Parsing component. Successful exploitation by a remote attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email, or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8581

**Description**
A vulnerability is present in some versions of Microsoft Windows.

**Observation**
Microsoft Windows is a popular operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Win32k component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8580

**Description**
A vulnerability is present in some versions of Microsoft Windows.

**Observation**
Microsoft Windows is a popular operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Win32k component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8578

**Description**
A vulnerability is present in some versions of Microsoft Windows.

**Observation**
Microsoft Windows is a popular operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Win32k component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

Description
A vulnerability is present in some versions of Microsoft Windows.

Observation
Microsoft Windows is a popular operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Win32k component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8486

Description
A vulnerability is present in some versions of Microsoft Windows.

Observation
Microsoft Windows is a popular operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Win32k component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8467

Description
A vulnerability is present in some versions of Microsoft Windows.

Observation
Microsoft Windows is a popular operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Win32k component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8559
Description
A vulnerability in some versions of Microsoft Exchange could lead to privilege escalation.

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

The flaw exists when Windows improperly handles calls to Advanced Local Procedure Call. Successful exploitation could allow a local user to gain elevated privileges.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8560

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

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

The flaw exists when Microsoft Exchange Outlook Web Access (OWA) fails to properly handle web requests. Successful exploitation could allow a local user to gain elevated privileges.

22092 - (MSPT-Jul2017) Microsoft Windows Explorer Denial of Service (CVE-2017-8587)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8587

Description
A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

Observation
A vulnerability in some versions of Microsoft Windows could lead to a denial of service.

The flaw exists when Windows Explorer attempts to open a non-existent file. Successful exploitation by a remote attacker could result in a denial of service condition.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8566

Description
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.

Observation
A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the IME component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8621

**Description**
A vulnerability in some versions of Microsoft Exchange could lead to information disclosure.

**Observation**
A vulnerability in some versions of Microsoft Exchange could lead to information disclosure.

The flaw occurs in Microsoft Exchange and could lead to spoofing. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.


Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8569

**Description**
A vulnerability in some versions of Microsoft SharePoint Server could lead to privilege escalation.

**Observation**
A vulnerability in some versions of Microsoft Sharepoint Server could lead to privilege escalation.

The flaw exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server. Successful exploitation could allow a local user to gain elevated privileges.


Category: Windows Host Assessment -> Patches and Hotfixes (CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8556

**Description**
A vulnerability is present in some versions of Microsoft Windows.

**Observation**
Microsoft Windows is a popular operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Graphics component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

Description
A vulnerability is present in some versions of Microsoft Windows.

Observation
Microsoft Windows is a popular operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Graphics component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8574

Description
A vulnerability is present in some versions of Microsoft Windows.

Observation
Microsoft Windows is a popular operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Graphics component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-0243

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 exists in Microsoft Office software when the software fails to properly handle objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8501
A vulnerability in some versions of Microsoft Office could lead to remote code execution.

The flaw exists in Microsoft Office software when the software fails to properly handle objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8502

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

The flaw exists in Microsoft Office software when the software fails to properly handle objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8570

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

The flaw exists in Microsoft Office software when the software fails to properly handle objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8563

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation.
Observation
Windows is a popular operation system developed by Microsoft.

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Kerberos component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-0170

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

Observation
Windows is a popular operation system developed by Microsoft.

A vulnerability in some versions of Microsoft Windows could lead to information disclosure. The flaw lies in the Performance Monitor component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8495

Description
A vulnerability in some versions of Microsoft Windows could lead to security bypass.

Observation
Windows is a popular operation system developed by Microsoft.

A vulnerability in some versions of Microsoft Windows could lead to security bypass. The flaw lies in the Kerberos component. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8557

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

Observation
Windows is a popular operation system developed by Microsoft.
A vulnerability in some versions of Microsoft Windows could lead to information disclosure. The flaw lies in the System Information Console component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8561

**Description**

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

**Observation**

Windows is a popular operation system developed by Microsoft.

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8562

**Description**

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

**Observation**

Windows is a popular operation system developed by Microsoft.

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw exits when Windows improperly handles calls to Advanced Local Procedure Call. Successful exploitation could allow a local user to gain elevated privileges.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8564

**Description**

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

**Observation**

Windows is a popular operation system developed by Microsoft.

A vulnerability in some versions of Microsoft Windows could lead to information disclosure. The flaw lies in the Kernel component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: Medium
CVE: CVE-2017-8501

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 exists in Microsoft Office software when the software fails to properly handle objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.


Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8592

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

Observation
Internet Explorer and Edge are Internet browsers developed by Microsoft.

An information disclosure vulnerability is present in some versions of Microsoft Browser. The flaw is due to improper handling of redirect requests. Successful exploitation could allow a remote attacker to obtain data that would otherwise be restricted to a destination web site of their choice.

22056 - (MSPT-Jul2017) Microsoft Browser Spoofing Vulnerability (CVE-2017-8602)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: Medium
CVE: CVE-2017-8602

Description
A spoofing vulnerability is present in some versions of Microsoft Internet Explorer and Edge.

Observation
Internet Explorer and Edge are Internet browsers developed by Microsoft.

A spoofing vulnerability is present in some versions of Microsoft Internet Explorer and Edge. The flaw is due to improper handling of HTTP responses. Successful exploitation could allow a remote attacker to spoof content or serve as a pivot to chain an attack with other vulnerabilities in web services.

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.

145424 - SuSE SLES 11 SP4 SUSE-SU-2017:1763-1 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2012-6706

Update Details
Risk is updated

145426 - SuSE SLES 12 SP2, SLED 12 SP2 SUSE-SU-2017:1716-1 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2012-6706

Update Details
Risk is updated

145432 - SuSE SLES 11 SP4 SUSE-SU-2017:1760-1 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: High
CVE: CVE-2012-6706

Update Details
Risk is updated

130799 - Debian Linux 8.0 DSA-3882-1 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium

Update Details
Risk is updated

130801 - Debian Linux 8.0 DSA-3883-1 Update Is Not Installed
Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5361

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

70086 - oracle.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.

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 2017 McAfee, Inc.
McAfee is a registered trademark of McAfee, Inc. and/or its affiliates