2017-SEP-12
FSL version 7.5.958

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

22374 - (MSPT-Sept2017) Microsoft Windows NetBIOS Remote Code Execution (CVE-2017-0161)

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

Risk Level: High

CVE: CVE-2017-0161

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 NetBIOS. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

22388 - (MSPT-Sept2017) Microsoft Internet Explorer Memory Corruption Remote Code Execution (CVE-2017-8749)

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

Risk Level: High

CVE: CVE-2017-8749

Description

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

Observation

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

The flaw is due to a memory corruption error. 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.

22404 - (MSPT-Sep2017) Microsoft Win32k Graphics Remote Code Execution Vulnerability (CVE-2017-8682)

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

Risk Level: High

CVE: CVE-2017-8682

Description

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

Observation

Windows is a popular operation system developed by Microsoft.

A vulnerability in some versions of Microsoft Windows could lead to remote code execution. The flaw occurs in the way that Windows font library handles embedded fonts. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

22415 - (MSPT-Sept2017) Microsoft Edge Memory Corruption Remote Code Execution (CVE-2017-11766)

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

Risk Level: High

CVE: CVE-2017-11766

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 is due to a memory corruption error. 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.

22436 - (MSPT-Sept2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-8752)

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

Risk Level: High

CVE: CVE-2017-8752

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

22437 - (MSPT-Sept2017) Microsoft .NET Library Loading Remote Code Execution (CVE-2017-8759)

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

Risk Level: High

CVE: CVE-2017-8759

Description

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

Observation

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

The flaw is due to improper handling of untrusted input. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a malicious document or application.

22451 - (APSB17-28) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2017-11281, CVE-2017-11282

Description

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

Observation

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.

The update provided by Adobe bulletin APSB17-28 resolves these issues. The target system is missing this update.

22452 - (APSB17-28) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-11281, CVE-2017-11282

Description

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

Observation

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.

The update provided by Adobe bulletin APSB17-28 resolves these issues. The target system is missing this update.

22389 - (MSPT-Sept2017) Microsoft Windows Browser Remote Code Execution (CVE-2017-8750)

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

Risk Level: High

CVE: CVE-2017-8750

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 the way the Scripting Engine renders when handling objects in memory in Microsoft browsers. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploitation requires the user to open a malicious website, email or document.

22435 - (MSPT-Sept2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-8729)

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

Risk Level: High

CVE: CVE-2017-8729

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

22218 - (MSPT-Sep2017) Microsoft Office Memory Corruption Remote Code Execution (CVE-2017-8630)

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

Risk Level: High

CVE: CVE-2017-8630

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 is due to a memory corruption error. 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.

22354 - (MSPT-Sep2017) Microsoft Office Memory Corruption Remote Code Execution (CVE-2017-8631)

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

Risk Level: High

CVE: CVE-2017-8631

Description

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

Observation

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

The flaw lies in a memory corruption error. 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.

22355 - (MSPT-Sep2017) Microsoft Office Memory Corruption Remote Code Execution (CVE-2017-8632)

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

Risk Level: High

CVE: CVE-2017-8632

Description

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

Observation

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

The flaw lies in a memory corruption error. 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.

22356 - (MSPT-Sept2017) Microsoft Office Publisher Remote Code Execution (CVE-2017-8725)

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

Risk Level: High

CVE: CVE-2017-8725

Description

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

Observation

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

The flaw lies in the Publisher 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.

22366 - (MSPT-Sept2017) Microsoft Windows Hyper-V Denial of Service (CVE-2017-8704)

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

Risk Level: High

CVE: CVE-2017-8704

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 lies in the Hyper-V component. Successful exploitation by a remote attacker could result in a denial of service condition. The exploit requires the user to open a vulnerable website, email or document.

22367 - (MSPT-Sept2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-8748)

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

Risk Level: High

CVE: CVE-2017-8748

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 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.

22369 - (MSPT-Sept2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-8741)

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

Risk Level: High

CVE: CVE-2017-8741

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 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.

22371 - (MSPT-Sept2017) Microsoft Internet Explorer Memory Corruption Remote Code Execution (CVE-2017-8747)

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

Risk Level: High

CVE: CVE-2017-8747

Description

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

Observation

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

The flaw is due to a memory corruption error. 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.

22375 - (MSPT-Sept2017) Microsoft Windows Remote Desktop Protocol Remote Code Execution (CVE-2017-8714)

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

Risk Level: High

CVE: CVE-2017-8714

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 Remote Desktop VM Host Agent 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.

22376 - (MSPT-Sept2017) Microsoft Windows Device Guard Security Bypass (CVE-2017-8746)

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

Risk Level: High

CVE: CVE-2017-8746

Description

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

Observation

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

The flaw lies in the Device Guard 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.

22378 - (MSPT-Sep2017) Microsoft Win32k Elevation Of Privilege Vulnerability (CVE-2017-8675)

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

Risk Level: High

CVE: CVE-2017-8675

Description

An elevation of privilege vulnerability is present in some versions of Microsoft Windows.

Observation

Windows is a popular operation system developed by Microsoft.

An elevation of privilege vulnerability is present in some versions of Microsoft Windows. The flaw lies in how the Windows kernel-mode driver handles objects in memory. Successful exploitation could allow an attacker to execute processes with elevated privileges. Exploitation requires an attacker to gain access to the local system.

22380 - (MSPT-Sept2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-8719)

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

Risk Level: High

CVE: CVE-2017-8719

Description

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

Observation

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

The flaw lies in the Kernel component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

22383 - (MSPT-Sept2017) Microsoft Windows PDF Remote Code Execution (CVE-2017-8728)

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

Risk Level: High

CVE: CVE-2017-8728

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 PDF 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.

22385 - (MSPT-Sept2017) Microsoft Windows PDF Remote Code Execution (CVE-2017-8737)

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

Risk Level: High

CVE: CVE-2017-8737

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 PDF 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.

22386 - (MSPT-Sep2017) Microsoft Win32k Graphics Information Disclosure Vulnerability (CVE-2017-8683)

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

Risk Level: High

CVE: CVE-2017-8683

Description

An elevation of privilege vulnerability is present in some versions of Microsoft Windows.

Observation

Windows is a popular operation system developed by Microsoft.

An elevation of privilege vulnerability is present in some versions of Microsoft Windows. The flaw lies in how the Windows graphics component handles objects in memory. Successful exploitation could allow an attacker to execute processes with elevated privileges or retrieve sensitive data. Exploitation requires an attacker to gain access to the local system.

22390 - (MSPT-Sept2017) Microsoft Office PowerPoint Remote Code Execution (CVE-2017-8742)

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

Risk Level: High

CVE: CVE-2017-8742

Description

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

Observation

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

The flaw lies in the Power Point 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.

22400 - (MSPT-Sep2017) Microsoft Win32k Elevation Of Privilege Vulnerability (CVE-2017-8720)

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

Risk Level: High

CVE: CVE-2017-8720

Description

An elevation of privilege vulnerability is present in some versions of Microsoft Windows.

Observation

Windows is a popular operation system developed by Microsoft.

An elevation of privilege vulnerability is present in some versions of Microsoft Windows. The flaw lies in how the Win32k handles objects in memory. Successful exploitation could allow an attacker to execute processes with elevated privileges. Exploitation requires an attacker to gain access to the local system.

22401 - (MSPT-Sept2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-8738)

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

Risk Level: High

CVE: CVE-2017-8738

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.

22402 - (MSPT-Sept2017) Microsoft Edge Memory Corruption Remote Code Execution (CVE-2017-8755)

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

Risk Level: High

CVE: CVE-2017-8755

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. 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.

22403 - (MSPT-Sept2017) Microsoft Edge Memory Corruption Remote Code Execution (CVE-2017-8756)

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

Risk Level: High

CVE: CVE-2017-8756

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. 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.

22405 - (MSPT-Sep2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-8753)

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

Risk Level: High

CVE: CVE-2017-8753

Description

A memory corruption vulnerability is present in some versions of Microsoft Edge.

Observation

Microsoft Edge is the new default web browser in Windows 10.

A memory corruption vulnerability is present in some versions of Microsoft Edge. The flaw lies in the JavaScript engine in handling objects in memory. Successful exploitation could allow an attacker to corrupt memory and execute code in the context of the current user by convincing the user to visit a malicious website.

22410 - (MSPT-Sept2017) Microsoft Office PowerPoint Remote Code Execution (CVE-2017-8743)

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

Risk Level: High

CVE: CVE-2017-8743

Description

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

Observation

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

The flaw lies in the PowerPoint 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.

22414 - (MSPT-Sept2017) Microsoft Edge Memory Corruption Remote Code Execution (CVE-2017-8751)

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

Risk Level: High

CVE: CVE-2017-8751

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 is due to a memory corruption error. 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.

22418 - (MSPT-Sep2017) Microsoft Graphics Component Information Disclosure Vulnerability (CVE-2017-8695)

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

Risk Level: High

CVE: CVE-2017-8695

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 an attacker to retrieve sensitive data from the target system.

22421 - (MSPT-Sep2017) Microsoft Edge Remote Code Execution Vulnerability (CVE-2017-8757)

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

Risk Level: High

CVE: CVE-2017-8757

Description

A vulnerability is present in some versions of Microsoft Edge.

Observation

Microsoft Edge is the Windows 10 browser by default.

A vulnerability is present in some versions of Microsoft Edge. The flaw is due to how this software handles objects in memory. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22422 - (MSPT-Sep2017) Scripting Engine Memory Corruption Vulnerability (CVE-2017-11764)

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

Risk Level: High

CVE: CVE-2017-11764

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

A remote code execution vulnerability is present in some versions of Microsoft Edge. The flaw lies in the Scripting Engine. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22423 - (MSPT-Sept2017) Microsoft Windows DHCP Server Remote Code Execution (CVE-2017-8686)

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

Risk Level: High

CVE: CVE-2017-8686

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 DHCP Server component. Successful exploitation by an attacker could result in the execution of arbitrary code. Exploitation is possible when attacker can send specially crafted packets to a DHCP fail-over server.

22428 - (MSPT-Sep2017) Microsoft Office Memory Corruption Vulnerability (CVE-2017-8744)

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

Risk Level: High

CVE: CVE-2017-8744

Description

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

Observation

Microsoft Office is a popular office products suite.

A remote code execution vulnerability is present in some versions of Microsoft Office. The flaw is due to the bad memory object handling of the Microsoft Office software. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22429 - (MSPT-Sep2017) Microsoft Office Remote Code Execution Vulnerability (CVE-2017-8567)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-8567

Description

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

Observation

Microsoft Office is a popular office products suite.

A remote code execution vulnerability is present in some versions of Microsoft Office. The flaw is due to a bad memory object handling of the Microsoft Office software. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22431 - (MSPT-Sept2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-8649)

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

Risk Level: High

CVE: CVE-2017-8649

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 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 malicious website, email or document.

22432 - (MSPT-Sept2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-8660)

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

Risk Level: High

CVE: CVE-2017-8660

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

22446 - (MSPT-Sep2017) Microsoft Office Memory Corruption Remote Code Execution (CVE-2017-8631)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-8631

Description

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

Observation

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

The flaw lies in a memory corruption error. 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.

22447 - (MSPT-Sep2017) Microsoft Office Memory Corruption Remote Code Execution (CVE-2017-8632)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-8632

Description

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

Observation

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

The flaw lies in a memory corruption error. 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.

22346 - (MSPT-Sept2017) Microsoft Office Sharepoint Privilege Escalation (CVE-2017-8745)

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

Risk Level: Medium

CVE: CVE-2017-8745

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 is due to failure to properly sanitize a specially crafted web request. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

22360 - (MSPT-Sept2017) Microsoft Windows Security Security Bypass (CVE-2017-8716)

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

Risk Level: Medium

CVE: CVE-2017-8716

Description

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

Observation

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

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

22361 - (MSPT-Sept2017) Microsoft Windows Hyper-V Information Disclosure (CVE-2017-8713)

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

Risk Level: Medium

CVE: CVE-2017-8713

Description

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

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.
The flaw lies in the Hyper-V component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22362 - (MSPT-Sept2017) Microsoft Windows Hyper-V Information Disclosure (CVE-2017-8712)

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

Risk Level: Medium

CVE: CVE-2017-8712

Description

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

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.
The flaw lies in the Hyper-V component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22363 - (MSPT-Sept2017) Microsoft Windows Hyper-V Information Disclosure (CVE-2017-8711)

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

Risk Level: Medium

CVE: CVE-2017-8711

Description

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

Observation

A vulnerability in some versions of Microsoft Windows could lead to information disclosure.
The flaw lies in the Hyper-V component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22364 - (MSPT-Sept2017) Microsoft Windows Hyper-V Information Disclosure (CVE-2017-8707)

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

Risk Level: Medium

CVE: CVE-2017-8707

Description

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

Observation

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

The flaw lies in the Hyper-V component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22365 - (MSPT-Sept2017) Microsoft Windows Hyper-V Information Disclosure (CVE-2017-8706)

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

Risk Level: Medium

CVE: CVE-2017-8706

Description

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

Observation

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

The flaw lies in the Hyper-V component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22368 - (MSPT-Sept2017) Microsoft Internet Explorer Browser Information Disclosure (CVE-2017-8736)

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

Risk Level: Medium

CVE: CVE-2017-8736

Description

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

Observation

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

The flaw is due to improper parent domain verification in certain functionality. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22370 - (MSPT-Sept2017) Microsoft Internet Explorer Spoofing Vulnerability (CVE-2017-8733)

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

Risk Level: Medium

CVE: CVE-2017-8733

Description

A spoofing vulnerability is present in some version Microsoft Internet Explorer.

Observation

A spoofing vulnerability is present in some version Microsoft Internet Explorer.

The flaw is due to improper handling of specific HTML content. Successful exploitation by a remote attacker could trick a victim into believing that the user was visiting a legitimate website. The exploit requires the user to open a vulnerable website, email or document.

22372 - (MSPT-Sept2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-8679)

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

Risk Level: Medium

CVE: CVE-2017-8679

Description

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

Observation

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

The flaw lies in the Windows kernel. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the user to log on to an affected system and run a specially crafted application.

22377 - (MSPT-Sept2017) Microsoft Windows Uniscribe Remote Code Execution (CVE-2017-8692)

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

Risk Level: Medium

CVE: CVE-2017-8692

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 Uniscribe 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.

22379 - (MSPT-Sep2017) Microsoft Win32k Information Disclosure Vulnerability (CVE-2017-8677)

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

Risk Level: Medium

CVE: CVE-2017-8677

Description

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

Observation

Windows is a popular operation system developed by Microsoft.

An information disclosure vulnerability is present in some versions of Microsoft Windows. The flaw lies in how the Windows GDI component handles objects in memory. Successful exploitation could allow an attacker to obtain restricted information. Exploitation requires an attacker to execute a specially crafted application.

22381 - (MSPT-Sep2017) Microsoft Win32k Information Disclosure Vulnerability (CVE-2017-8678)

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

Risk Level: Medium

CVE: CVE-2017-8678

Description

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

Observation

Windows is a popular operation system developed by Microsoft.

An information disclosure vulnerability is present in some versions of Microsoft Windows. The flaw lies in how the Windows kernel handles objects in memory. Successful exploitation could allow an attacker to obtain restricted information. Exploitation requires an attacker to execute a specially crafted application.

22382 - (MSPT-Sep2017) Win32k Information Disclosure Vulnerability (CVE-2017-8680)

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

Risk Level: Medium

CVE: CVE-2017-8680

Description

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

Observation

Windows is a popular operation system developed by Microsoft.

An information disclosure vulnerability is present in some versions of Microsoft Windows. The flaw lies in how the Windows GDI component handles objects in memory. Successful exploitation could allow an attacker to obtain restricted information. Exploitation requires an attacker to execute a specially crafted application.

22384 - (MSPT-Sep2017) Microsoft Win32k Information Disclosure Vulnerability (CVE-2017-8681)

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

Risk Level: Medium

CVE: CVE-2017-8681

Description

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

Observation

Windows is a popular operation system developed by Microsoft.

An information disclosure vulnerability is present in some versions of Microsoft Windows. The flaw lies in how the Windows GDI component handles objects in memory. Successful exploitation could allow an attacker to obtain restricted information. Exploitation requires an attacker to execute a specially crafted application.

22392 - (MSPT-Sept2017) Microsoft Edge Memory Corruption Remote Code Execution (CVE-2017-8731)

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

Risk Level: Medium

CVE: CVE-2017-8731

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 is due to a memory corruption error. 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.

22393 - (MSPT-Sept2017) Microsoft Edge Memory Corruption Remote Code Execution (CVE-2017-8734)

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

Risk Level: Medium

CVE: CVE-2017-8734

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 is due to a memory corruption error. 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.

22394 - (MSPT-Sept2017) Microsoft Edge Spoofing Information Disclosure (CVE-2017-8735)

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

Risk Level: Medium

CVE: CVE-2017-8735

Description

A spoofing vulnerability is present in some version Microsoft Edge.

Observation

A spoofing vulnerability is present in some version Microsoft Edge.

The flaw is due to Microsoft EDGE does not properly parse of http content. Successful exploitation by a remote attacker could trick a victim into believing that the user was visiting a legitimate website. The exploit requires the user to open a vulnerable website, email or document.

22395 - (MSPT-Sept2017) Microsoft Windows Scripting Engine Information Disclosure (CVE-2017-8739)

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

Risk Level: Medium

CVE: CVE-2017-8739

Description

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

Observation

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

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

22396 - (MSPT-Sep2017) Win32k GDI Information Disclosure Vulnerability (CVE-2017-8684)

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

Risk Level: Medium

CVE: CVE-2017-8684

Description

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

Observation

Windows is a popular operation system developed by Microsoft.

An information disclosure vulnerability is present in some versions of Microsoft Windows. The flaw lies in how the Windows GDI component handles objects in memory. Successful exploitation could allow an attacker to obtain restricted information. Exploitation requires an attacker to execute a specially crafted application.

22397 - (MSPT-Sept2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-8740)

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

Risk Level: Medium

CVE: CVE-2017-8740

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.

22398 - (MSPT-Sep2017) Win32k GDI Information Disclosure Vulnerability (CVE-2017-8685)

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

Risk Level: Medium

CVE: CVE-2017-8685

Description

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

Observation

Windows is a popular operation system developed by Microsoft.

An information disclosure vulnerability is present in some versions of Microsoft Windows. The flaw lies in how the Windows GDI

component handles objects in memory. Successful exploitation could allow an attacker to obtain restricted information. Exploitation requires an attacker to execute a specially crafted application.

22399 - (MSPT-Sep2017) Microsoft Win32k Information Disclosure Vulnerability (CVE-2017-8687)

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

Risk Level: Medium

CVE: CVE-2017-8687

Description

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

Observation

Windows is a popular operation system developed by Microsoft.

An information disclosure vulnerability is present in some versions of Microsoft Windows. The flaw lies in how the Windows kernel handles memory address. Successful exploitation could allow an attacker to obtain restricted information. Exploitation requires an attacker to execute a specially crafted application.

22406 - (MSPT-Sep2017) Microsoft Edge Security Feature Bypass Vulnerability (CVE-2017-8754)

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

Risk Level: Medium

CVE: CVE-2017-8754

Description

A security feature bypass vulnerability is present in some versions of Microsoft Edge.

Observation

Microsoft Edge is the new default web browser in Windows 10.

A security feature bypass vulnerability is present in some versions of Microsoft Edge. The flaw occurs when Microsoft Edge CSP improperly validates documents. Successful exploitation could allow an attacker to trick a user into loading a web page with malicious content.

22407 - (MSPT-Sept2017) Microsoft Windows GDI+ Information Disclosure (CVE-2017-8688)

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

Risk Level: Medium

CVE: CVE-2017-8688

Description

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

Observation

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

The flaw lies in the GDI+ component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to log on to an affected system and run a specially crafted application.

22408 - (MSPT-Sept2017) Microsoft Windows GDI+ Information Disclosure (CVE-2017-8676)

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

Risk Level: Medium

CVE: CVE-2017-8676

Description

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

Observation

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

The flaw lies in the GDI+ component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to log on to an affected system and run a specially crafted application.

22411 - (MSPT-Sept2017) Microsoft Office SharePoint Privilege Escalation (CVE-2017-8629)

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

Risk Level: Medium

CVE: CVE-2017-8629

Description

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

Observation

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

The flaw lies in the SharePoint 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.

22412 - (MSPT-Sept2017) Microsoft Exchange Cross-Site Scripting Information Disclosure (CVE-2017-8758)

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

Risk Level: Medium

CVE: CVE-2017-8758

Description

A cross-site scripting vulnerability is present in some versions of Microsoft Exchange.

Observation

A cross-site scripting vulnerability is present in some versions of Microsoft Exchange.

The flaw is due to improper validating web requests. Successful exploitation could allow a remote attacker to inject arbitrary script, and obtain sensitive information. The exploit requires the user to click a maliciously crafted link.

22413 - (MSPT-Sept2017) Microsoft Exchange Memory Corruption Information Disclosure (CVE-2017-11761)

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

Risk Level: Medium

CVE: CVE-2017-11761

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 is due to improper handling of tags in Calendar-related messages. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

22416 - (MSPT-Sept2017) Microsoft Windows Error Reporting Privilege Escalation (CVE-2017-8702)

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

Risk Level: Medium

CVE: CVE-2017-8702

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 Error Reporting 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.

22417 - (MSPT-Sept2017) Microsoft Windows System Information Console Information Disclosure (CVE-2017-8710)

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

Risk Level: Medium

CVE: CVE-2017-8710

Description

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

Observation

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

The flaw lies in the System Information Console component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22420 - (MSPT-Sep2017) Microsoft Bluetooth Driver Spoofing Vulnerability (CVE-2017-8628)

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

Risk Level: Medium

CVE: CVE-2017-8628

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 Bluetooth stack. Successful exploitation could allow an attacker to perform a man-in-the-middle attack, monitor and read the traffic before sending it on to the intended recipient.

22424 - (MSPT-Sept2017) Microsoft Windows Shell Remote Code Execution (CVE-2017-8699)

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

Risk Level: Medium

CVE: CVE-2017-8699

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 Windows Shell component. Successful exploitation by a remote attacker could result in the execution of arbitrary code in the context of the current user. The exploitation requires the user to open a specially crafted file delivered via malicious website, email or document.

22425 - (MSPT-Sept2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-8709)

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

Risk Level: Medium

CVE: CVE-2017-8709

Description

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

Observation

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

22426 - (MSPT-Sept2017) Microsoft Edge Chakra Information Disclosure (CVE-2017-8597)

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

Risk Level: Medium

CVE: CVE-2017-8597

Description

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

Observation

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

The flaw lies in the Chakra component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22430 - (MSPT-Sept2017) Microsoft Edge Chakra Information Disclosure (CVE-2017-8648)

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

Risk Level: Medium

CVE: CVE-2017-8648

Description

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

Observation

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

The flaw lies in the Chakra component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a malicious website, email or document.

22453 - (MSPT-Sept2017) Microsoft Windows GDI+ Information Disclosure (CVE-2017-8676)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-8676

Description

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

Observation

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

The flaw lies in the GDI+ component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to log on to an affected system and run a specially crafted application.

22373 - (MSPT-Sept2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-8708)

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

Risk Level: Medium

CVE: CVE-2017-8708

Description

A vulnerability is present in some versions of Microsoft Windows.

Observation

Microsoft Windows is a popular operation system.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Windows kernel. Successful exploitation by an attacker could result in the disclosure of sensitive information. The exploit requires the user to log on to an affected system and run a specially crafted application.

22427 - (MSPT-Sept2017) Microsoft Edge Clipboard Information Disclosure (CVE-2017-8643)

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

Risk Level: Medium

CVE: CVE-2017-8643

Description

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

Observation

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

The flaw lies in the Clipboard component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

22433 - (MSPT-Sept2017) Microsoft Edge Security Security Bypass (CVE-2017-8723)

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

Risk Level: Medium

CVE: CVE-2017-8723

Description

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

Observation

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

The flaw is due to a failure in Content Security Policy (CSP) to properly validate certain specially crafted documents. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. The exploitation requires the user to open a malicious website, email or document.

22434 - (MSPT-Sept2017) Microsoft Edge Spoofing Information Disclosure (CVE-2017-8724)

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

Risk Level: Medium

CVE: CVE-2017-8724

Description

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

Observation

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

The flaw is due to a failure in Microsoft Edge in properly parsing HTTP content. Successful exploitation by a remote attacker could result in redirecting the user to a specially crafted website. The exploitation requires the user to open a specially crafted URL in a malicious website, email or document.

22419 - (MSPT-Sep2017) Microsoft Graphics Component Remote Code Execution Vulnerability (CVE-2017-8696)

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

Risk Level: Informational

CVE: CVE-2017-8696

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 is due to how Windows Uniscribe handles objects in memory. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

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.

181433 - FreeBSD strongswan Denial-of-service And Potential Remote Code Execution Vulnerability (55363e65-0e71-11e5-8027-00167671dd1d)

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

Risk Level: High

CVE: CVE-2015-3991

Update Details

Risk is updated

178274 - Gentoo Linux GLSA-201612-39 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes

Risk Level: Medium

CVE: CVE-2016-0634

Update Details

Risk is updated

182432 - FreeBSD gdk-pixbuf Multiple Vulnerabilities (5a1f1a86-8f4c-11e7-b5af-a4badb2f4699)

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

Risk Level: Medium

CVE: CVE-2017-2862, CVE-2017-2870

Update Details

Risk is updated

191169 - Fedora Linux 24 FEDORA-2016-a822b472c4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-0634

Update Details

Risk is updated

191176 - Fedora Linux 23 FEDORA-2016-62e6c462ef Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-0634

Update Details
Risk is updated

191179 - Fedora Linux 25 FEDORA-2016-eda100d886 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-0634

Update Details
Risk is updated

192603 - Fedora Linux 26 FEDORA-2017-382c240580 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-14032

Update Details
Risk is updated

130845 - Debian Linux 8.0, 9.0 DSA-3940-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-12836

Update Details
Risk is updated

181550 - FreeBSD froxlor Database Password Information Leak (9ee72858-4159-11e5-93ad-002590263bf5)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-5959

Update Details
Risk is updated

185847 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3399-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-12836

Update Details

Risk is updated

185866 - Ubuntu Linux 16.04, 17.04 USN-3407-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-11424

Update Details

Risk is updated

192576 - Fedora Linux 25 FEDORA-2017-97eb475d93 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12836

Update Details

Risk is updated

192581 - Fedora Linux 26 FEDORA-2017-e5a78c5ca9 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12836

Update Details

Risk is updated

93346 - Mandriva Linux MBS1 MDVSA-2014-135 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4616

Update Details

Risk is updated

142303 - SuSE Linux 12.3, 13.1 openSUSE-SU-2014:0890-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4616

Update Details

Risk is updated

170342 - Amazon Linux AMI ALAS-2014-374 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2014-4616

Update Details
Risk is updated

170378 - Amazon Linux AMI ALAS-2014-380 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-4616

Update Details
Risk is updated

188034 - Fedora Linux 20 FEDORA-2014-7800 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-4616

Update Details
Risk is updated

188086 - Fedora Linux 19 FEDORA-2014-7772 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-4616

Update Details
Risk is updated

188091 - Fedora Linux 19 FEDORA-2014-8035 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-4616

Update Details
Risk is updated

188444 - Fedora Linux 21 FEDORA-2014-14208 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-4616

Update Details
Risk is updated

188449 - Fedora Linux 20 FEDORA-2014-14245 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4616

Update Details

Risk is updated

188499 - Fedora Linux 19 FEDORA-2014-14257 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-4616

Update Details

Risk is updated

188965 - Fedora Linux 21 FEDORA-2015-1711 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-0233

Update Details

Risk is updated

70014 - netbios-helpers.fasl3.inc

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

Risk Level: Informational

CVE: CVE-MAP-NOMATCH

Update Details

FASLScript is updated

HOW TO UPDATE

FS1000 APPLIANCE customers should follow the instructions for Enterprise/Professional customers, below. In addition, we strongly urge all appliance customers to authorize and install any Windows Update critical patches. The appliance will auto-download any critical updates but will wait for your explicit authorization before installing.

FOUNDSTONE ENTERPRISE and PROFESSIONAL customers may obtain these new scripts using the FSUpdate Utility by selecting "FoundScan Update" on the help menu. Make sure that you have a valid FSUpdate username and password. The new vulnerability scripts will be automatically included in your scans if you have selected that option by right-clicking the selected vulnerability category and checking the "Run New Checks" checkbox.

MANAGED SERVICE CUSTOMERS already have the newest update applied to their environment. The new vulnerability scripts will be automatically included when your scans are next scheduled, provided the Run New Scripts option has been turned on.

MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

http://www.mcafee.com/us/about/contact/index.html

Non-US customers - Select your country from the list of Worldwide Offices.