2020-JAN-17
FSL version 7.6.144

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

25951 - (MSPT-Jun2020) Microsoft Internet Explorer Improperly Handles Objects In Memory Remote Code Execution (CVE-2020-0640)

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

Risk Level: High

CVE: CVE-2020-0640

Description

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

Observation

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

The flaw lies in improperly handles objects in memory. 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.

25952 - (MSPT-Jun2020) Microsoft Win32k Improperly Handles Objects In Memory Privilege Escalation (CVE-2020-0624)

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

Risk Level: High

CVE: CVE-2020-0624

Description

A vulnerability in some versions of Microsoft Win32k could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Win32k could lead to privilege escalation.

The flaw lies in improperly handles objects in memory. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25954 - (MSPT-Jan2020) Microsoft win32k Improperly Provides Kernel Information Disclosure (CVE-2020-0608)

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

Risk Level: High

CVE: CVE-2020-0608

Description

A vulnerability in some versions of Microsoft win32k could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft win32k could lead to information disclosure.

The flaw lies in improperly provided kernel information. 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.

25955 - (MSPT-Jan2020) Microsoft Search Indexer Improperly Handles Objects in Memory Privilege Escalation (CVE-2020-0613)

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

Risk Level: High

CVE: CVE-2020-0613

Description

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

Observation

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

The flaw lies in improper handling of memory objects. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25956 - (MSPT-Jan2020) Microsoft Search Indexer Improperly Handles Objects In Memory Privilege Escalation (CVE-2020-0623)

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

Risk Level: High

CVE: CVE-2020-0623

Description

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

Observation

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

The flaw lies in improper handling of memory objects. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25958 - (MSPT-Jan2020) Microsoft Search Indexer Improperly Handles Objects In Memory Privilege Escalation (CVE-2020-0625)

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

Risk Level: High

CVE: CVE-2020-0625

Description

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

Observation

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

The flaw lies in improper handling of memory objects. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25959 - (MSPT-Jan2020) Microsoft Search Indexer Improperly Handles Objects In Memory Privilege Escalation (CVE-2020-0626)

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

Risk Level: High

CVE: CVE-2020-0626

Description

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

Observation

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

The flaw lies in improper handling of memory objects. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25960 - (MSPT-Jan2020) Microsoft Search Indexer Improperly Handles Objects In Memory Privilege Escalation (CVE-2020-0627)

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

Risk Level: High

CVE: CVE-2020-0627

Description

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

Observation

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

The flaw lies in improper handling of memory objects. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25961 - (MSPT-Jan2020) Microsoft Search Indexer Improperly Handles Objects In Memory Privilege Escalation (CVE-2020-0628)

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

Risk Level: High

CVE: CVE-2020-0628

Description

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

Observation

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

The flaw lies in improperly handles objects in memory. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25981 - (MSPT-Jan2020) Microsoft CryptoAPI ECC Certificates Spoofing (CVE-2020-0601)

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

Risk Level: High

CVE: CVE-2020-0601

Description

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

Observation

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

The flaw lies in the ECC Certificates component. Successful exploitation by a remote attacker could result in spoofing. The exploit requires the user to open a vulnerable website, email or document.

25986 - (MSPT-Jan2020) Microsoft Excel Remote Code Execution Vulnerability (CVE-2020-0650)

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

Risk Level: High

CVE: CVE-2020-0650

Description

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

Observation

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

The flaw lies in improper handling of objects in memory. Successful exploitation by an attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25987 - (MSPT-Jan2020) Microsoft Excel Remote Code Execution Vulnerability (CVE-2020-0651)

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

Risk Level: High

CVE: CVE-2020-0651

Description

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

Observation

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

The flaw lies in improper handling of objects in memory. Successful exploitation by an attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25997 - (MSPT-Jan2020) Microsoft .NET Framework Remote Code Execution Vulnerability (CVE-2020-0605)

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

Risk Level: High

CVE: CVE-2020-0605

Description

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

Observation

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

The flaw lies in fails to check the source markup of a file. 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.

25998 - (MSPT-Jan2020) Microsoft .NET Framework Remote Code Execution Vulnerability (CVE-2020-0606)

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

Risk Level: High

CVE: CVE-2020-0606

Description

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

Observation

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

The flaw lies in fails to validate input properly. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

25999 - (MSPT-Jan2020) Microsoft .NET Framework Remote Code Execution Injection Vulnerability (CVE-2020-0646)

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

Risk Level: High

CVE: CVE-2020-0646

Description

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

Observation

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

The flaw lies in fails to validate input properly. 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.

25964 - (MSPT-Jan2020) Microsoft Hyper-V Virtual PCI Denial of Service (CVE-2020-0617)

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

Risk Level: High

CVE: CVE-2020-0617

Description

A vulnerability in some versions of Microsoft Hyper-V Virtual could lead to a denial of service.

Observation

A vulnerability in some versions of Microsoft Hyper-V Virtual could lead to a denial of service.

The flaw lies in the PCI component. Successful exploitation by a remote attacker could result in a denial of service condition. The exploit requires the attacker to have valid credentials to the vulnerable system.

25965 - (MSPT-Jan2020) Microsoft RDP Gateway Server Denial of Service (CVE-2020-0612)

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

Risk Level: High

CVE: CVE-2020-0612

Description

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

Observation

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

The flaw lies in the Gateway Server 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.

25968 - (MSPT-Jan2020) Microsoft ASP.NET Core Improperly Handles Web Requests Denial of Service (CVE-2020-0602)

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

Risk Level: High

CVE: CVE-2020-0602

Description

A vulnerability in some versions of Microsoft ASP.NET Core could lead to a denial of service.

Observation

A vulnerability in some versions of Microsoft ASP.NET Core could lead to a denial of service.

The flaw lies in improperly handles web requests. 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.

25969 - (MSPT-Jan2020) Microsoft ASP.NET Core Improperly Handle Objects in Memory Remote Code Execution (CVE-2020-0603)

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

Risk Level: High

CVE: CVE-2020-0603

Description

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

Observation

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

The flaw lies in improperly handles objects in memory. 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.

25971 - (MSPT-Jan2020) Microsoft Windows Graphics Component Information Disclosure (CVE-2020-0622)

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

Risk Level: High

CVE: CVE-2020-0622

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 Graphics 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.

25973 - (MSPT-Jan2020) Microsoft Windows Improperly Handles Hard Links Denial of Service (CVE-2020-0616)

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

Risk Level: High

CVE: CVE-2020-0616

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 improperly handles hard links. Successful exploitation by a remote attacker could result in a denial of service condition. The exploit requires the attacker to have valid credentials to the vulnerable system.

25978 - (MSPT-Jan2020) Microsoft Graphics Improperly Handle Objects in Memory Information Disclosure (CVE-2020-0607)

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

Risk Level: High

CVE: CVE-2020-0607

Description

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

Observation

A vulnerability in some versions of Microsoft Graphics 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 open a vulnerable website, email or document.

25982 - (MSPT-Jan2020) Microsoft Cryptographic Services Privilege Escalation (CVE-2020-0620)

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

Risk Level: High

CVE: CVE-2020-0620

Description

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

Observation

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

The flaw lies in improperly handles files. Successful exploitation could allow a local user to gain elevated privileges.

25984 - (MSPT-Jan2020) Microsoft Windows Subsystem For Linux Privilege Escalation (CVE-2020-0636)

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

Risk Level: High

CVE: CVE-2020-0636

Description

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

Observation

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

The flaw lies in the Linux 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.

25988 - (MSPT-Jan2020) Microsoft Office Memory Corruption Vulnerability (CVE-2020-0652)

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

Risk Level: High

CVE: CVE-2020-0652

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 improper handling of objects in memory. Successful exploitation by an attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

25989 - (MSPT-Jan2020) Windows Search Indexer Elevation of Privilege Vulnerability (CVE-2020-0631)

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

Risk Level: High

CVE: CVE-2020-0631

Description

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

Observation

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

The flaw lies in improper handling of objects in memory. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25990 - (MSPT-Jan2020) Windows Search Indexer Elevation of Privilege Vulnerability (CVE-2020-0632)

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

Risk Level: High

CVE: CVE-2020-0632

Description

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

Observation

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

The flaw lies in improper handling of objects in memory. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25991 - (MSPT-Jan2020) Windows Search Indexer Elevation of Privilege Vulnerability (CVE-2020-0633)

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

Risk Level: High

CVE: CVE-2020-0633

Description

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

Observation

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

The flaw lies in improper handling of objects in memory. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25992 - (MSPT-Jan2020) Microsoft Windows Remote Desktop Client Remote Code Execution (CVE-2020-0611)

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

Risk Level: High

CVE: CVE-2020-0611

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 Client 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.

25993 - (MSPT-Jan2020) Microsoft RDP Gateway Server Remote Code Execution (CVE-2020-0609)

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

Risk Level: High

CVE: CVE-2020-0609

Description

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

Observation

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

The flaw lies in the Gateway Server component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

25994 - (MSPT-Jan2020) Microsoft RDP Gateway Server Remote Code Execution (CVE-2020-0610)

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

Risk Level: High

CVE: CVE-2020-0610

Description

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

Observation

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

The flaw lies in the Gateway Server component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

25983 - (MSPT-Jan2020) Microsoft Windows Privilege Escalation (CVE-2020-0635)

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

Risk Level: Medium

CVE: CVE-2020-0635

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 improperly handling certain symbolic links. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25985 - (MSPT-Jan2020) Microsoft Office Online Spoofing Vulnerability (CVE-2020-0647)

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

Risk Level: Medium

CVE: CVE-2020-0647

Description

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

Observation

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

The flaw lies in not validate origin in cross-origin communications correctly. Successful exploitation by an attacker could result in spoofing. The exploit requires the attacker to have valid credentials to the vulnerable system.

25953 - (MSPT-Jan2020) Microsoft Win32k Improperly Handles Objects In Memory Privilege Escalation (CVE-2020-0642)

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

Risk Level: Medium

CVE: CVE-2020-0642

Description

A vulnerability in some versions of Microsoft Win32k could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Win32k could lead to privilege escalation.

The flaw lies in improperly handles objects in memory. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25957 - (MSPT-Jan2020) Microsoft Search Indexer Improperly Handles Objects in Memory Privilege Escalation (CVE-2020-0614)

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

Risk Level: Medium

CVE: CVE-2020-0614

Description

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

Observation

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

The flaw lies in improperly handles objects in memory. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25962 - (MSPT-Jan2020) Microsoft Search Indexer Improperly Handles Objects In Memory Privilege Escalation (CVE-2020-0629)

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

Risk Level: Medium

CVE: CVE-2020-0629

Description

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

Observation

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

The flaw lies in improperly handles objects in memory. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25963 - (MSPT-Jan2020) Microsoft Search Indexer Improperly Handles Objects In Memory Privilege Escalation (CVE-2020-0630)

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

Risk Level: Medium

CVE: CVE-2020-0630

Description

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

Observation

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

The flaw lies in improperly handles objects in memory. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

25966 - (MSPT-Jan2020) Microsoft Windows Web Access Information Disclosure (CVE-2020-0637)

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

Risk Level: Medium

CVE: CVE-2020-0637

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 Web Access 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.

25970 - (MSPT-Jan2020) Microsoft Windows Media Service Privilege Escalation (CVE-2020-0641)

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

Risk Level: Medium

CVE: CVE-2020-0641

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 Media Service 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.

25972 - (MSPT-Jan2020) Microsoft CLFS Update Notification Manager Privilege Escalation (CVE-2020-0638)

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

Risk Level: Medium

CVE: CVE-2020-0638

Description

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

Observation

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

The flaw lies in the Update Notification Manager 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.

25974 - (MSPT-Jan2020) Microsoft Windows GDI+ Information Disclosure (CVE-2020-0643)

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

Risk Level: Medium

CVE: CVE-2020-0643

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 attacker to have valid credentials to the vulnerable system.

25975 - (MSPT-Jan2020) Microsoft Windows 10 Third Party Filters Privilege Escalation (CVE-2020-0621)

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

Risk Level: Medium

CVE: CVE-2020-0621

Description

A vulnerability in some versions of Microsoft Windows 10 could lead to privilege escalation.

Observation

A vulnerability in some versions of Microsoft Windows 10 could lead to privilege escalation.

The flaw lies in the Third Party Filters 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.

25976 - (MSPT-Jan2020) Microsoft Windows Predictable Memory Section Names Privilege Escalation (CVE-2020-0644)

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

Risk Level: Medium

CVE: CVE-2020-0644

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 Predictable Memory Section Names 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.

25977 - (MSPT-Jan2020) Microsoft CLFS Improperly Handles Objects in Memory Information Disclosure (CVE-2020-0615)

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

Risk Level: Medium

CVE: CVE-2020-0615

Description

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

Observation

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

The flaw lies in improperly handles objects in memory. 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.

25979 - (MSPT-Jan2020) Microsoft Windows CLFS Privilege Escalation (CVE-2020-0634)

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

Risk Level: Medium

CVE: CVE-2020-0634

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 CLFS 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.

25980 - (MSPT-Jan2020) Microsoft CLFS Improperly Handles Objects In Memory Information Disclosure (CVE-2020-0639)

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

Risk Level: Medium

CVE: CVE-2020-0639

Description

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

Observation

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

The flaw lies in improperly handles objects in memory. 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.

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.