2018-FEB-13
FSL version 7.6.2

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

23071 - (MSPT-Feb2018) Microsoft Scripting Engine Remote Code Execution (CVE-2018-0834)

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

Risk Level: High

CVE: CVE-2018-0834

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.

23072 - (MSPT-Feb2018) Microsoft Scripting Engine Remote Code Execution (CVE-2018-0835)

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

Risk Level: High

CVE: CVE-2018-0835

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.

23083 - (MSPT-Feb2018) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2018-0837)

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

Risk Level: High

CVE: CVE-2018-0837

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.

23084 - (MSPT-Feb2018) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2018-0838)

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

Risk Level: High

CVE: CVE-2018-0838

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.

23086 - (MSPT-Feb2018) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2018-0856)

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

Risk Level: High

CVE: CVE-2018-0856

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.

23088 - (MSPT-Feb2018) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2018-0859)

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

Risk Level: High

CVE: CVE-2018-0859

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.

23105 - (MSPT-Feb2018) Microsoft Edge Memory Handling Information Disclosure (CVE-2018-0763)

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

Risk Level: High

CVE: CVE-2018-0763

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 a memory handling error. 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.

23108 - (MSPT-Feb2018) Microsoft Internet Explorer Scripting Engine Memory Corruption Vulnerability (CVE-2018-0866)

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

Risk Level: High

CVE: CVE-2018-0866

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 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.

23111 - (MSPT-Feb2018) Microsoft Windows StructuredQuery Remote Code Execution (CVE-2018-0825)

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

Risk Level: High

CVE: CVE-2018-0825

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 StructuredQuery 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.

23116 - (MSPT-Feb2018) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2018-0860)

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

Risk Level: High

CVE: CVE-2018-0860

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.

23117 - (MSPT-Feb2018) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2018-0861)

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

Risk Level: High

CVE: CVE-2018-0861

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.

23119 - (MSPT-Feb2018) Microsoft Browser Scripting Engine Remote Code Execution (CVE-2018-0840)

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

Risk Level: High

CVE: CVE-2018-0840

Description

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

Observation

A vulnerability in some versions of Microsoft 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.

23130 - (APSB18-02) Vulnerabilities In Adobe Acrobat and Reader

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

Risk Level: High

CVE: CVE-2018-4872, CVE-2018-4879, CVE-2018-4880, CVE-2018-4881, CVE-2018-4882, CVE-2018-4883, CVE-2018-4884, CVE-2018-4885, CVE-2018-4886, CVE-2018-4887, CVE-2018-4888, CVE-2018-4889, CVE-2018-4890, CVE-2018-4891, CVE-2018-4892, CVE-2018-4893, CVE-2018-4894, CVE-2018-4895, CVE-2018-4896, CVE-2018-4897, CVE-2018-4898, CVE-2018-4899, CVE-2018-4900, CVE-2018-4901, CVE-2018-4902, CVE-2018-4903, CVE-2018-4904, CVE-2018-4905, CVE-2018-4906, CVE-2018-4907, CVE-

2018-4908, CVE-2018-4909, CVE-2018-4910, CVE-2018-4911, CVE-2018-4912, CVE-2018-4913, CVE-2018-4914, CVE-2018-4915, CVE-2018-4916, CVE-2018-4917, CVE-2018-4918

Description

Multiple vulnerabilities are present in some versions of Adobe Reader and Acrobat.

Observation

Adobe Reader and Acrobat are popular applications used to handle PDF files.

Multiple vulnerabilities are present in some versions of Adobe Reader and Acrobat. The flaws occur due to several memory corruption issues. Successful exploitation could allow an attacker to bypass security access restrictions or remotely execute arbitrary code on the target system.

The update provided by Adobe bulletin APSB18-02 resolves these issues. The target system appears to be missing this update.

23062 - (MSPT-Feb2018) Microsoft Office Outlook Memory Corruption Remote Code Execution (CVE-2018-0852)

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

Risk Level: High

CVE: CVE-2018-0852

Description

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

Observation

A vulnerability in some versions of Microsoft Office Outlook 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.

23075 - (MSPT-Feb2018) Microsoft Office Memory Corruption Remote Code Execution (CVE-2018-0851)

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

Risk Level: High

CVE: CVE-2018-0851

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.

23085 - (MSPT-Feb2018) Microsoft Edge Memory Corruption Information Disclosure (CVE-2018-0839)

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

Risk Level: High

CVE: CVE-2018-0839

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 a memory corruption error. 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.

23087 - (MSPT-Feb2018) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2018-0857)

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

Risk Level: High

CVE: CVE-2018-0857

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.

23090 - (MSPT-Feb2018) Microsoft Windows Common Log File System Privilege Escalation (CVE-2018-0846)

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

Risk Level: High

CVE: CVE-2018-0846

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 Common Log File System 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.

23094 - (MSPT-Feb2018) Microsoft Windows Kernel Privilege Escalation (CVE-2018-0831)

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

Risk Level: High

CVE: CVE-2018-0831

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 Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

23097 - (MSPT-Feb2018) Microsoft Windows Kernel Remote Code Execution (CVE-2018-0842)

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

Risk Level: High

CVE: CVE-2018-0842

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 Kernel component. Successful exploitation by a remote attacker could result in the execution of arbitrary code.The exploit requires the attacker to have valid credentials to the vulnerable system.

23101 - (MSPT-Feb2018) Microsoft Windows AppContainer Privilege Escalation (CVE-2018-0821)

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

Risk Level: High

CVE: CVE-2018-0821

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 AppContainer component.Successful exploitation could allow a local user to gain elevated privileges.The exploit requires the attacker to log in the vulnerable system first.

23103 - (MSPT-Feb2018) Microsoft Windows NTFS Global Reparse Privilege Escalation (CVE-2018-0822)

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

Risk Level: High

CVE: CVE-2018-0822

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 NTFS Global Reparse component.Successful exploitation could allow a local user to gain elevated privileges.The exploit requires the attacker to log in the vulnerable system.

23104 - (MSPT-Feb2018) Microsoft Windows Named Pipe File System Privilege Escalation (CVE-2018-0823)

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

Risk Level: High

CVE: CVE-2018-0823

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 Named Pipe File System component.Successful exploitation could allow a local user to gain elevated privileges.The exploit requires the attacker to log in the vulnerable system.

23107 - (MSPT-Feb2018) Microsoft Windows Kernel Privilege Escalation (CVE-2018-0742)

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

Risk Level: High

CVE: CVE-2018-0742

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 Kernel component.Successful exploitation could allow a local user to gain elevated privileges.The exploit requires the attacker to log in the vulnerable system.

23118 - (MSPT-Feb2018) Microsoft Windows Kernel Privilege Escalation (CVE-2018-0820)

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

Risk Level: High

CVE: CVE-2018-0820

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 Kernel component.Successful exploitation could allow a local user to gain elevated privileges.The exploit requires the attacker to log in the vulnerable system.

23070 - (MSPT-Feb2018) Microsoft Windows Scripting Engine Information Disclosure (CVE-2018-0847)

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

Risk Level: Medium

CVE: CVE-2018-0847

Description

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

Observation

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

The flaw lies in a memory corruption error. 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.

23063 - (MSPT-Feb2018) Microsoft Office Outlook Incoming Message Privilege Escalation (CVE-2018-0850)

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

Risk Level: Medium

CVE: CVE-2018-0850

Description

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

Observation

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

The flaw lies in the Incoming Message 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.

23073 - (MSPT-Feb2018) Microsoft Windows Kernel Information Disclosure (CVE-2018-0843)

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

Risk Level: Medium

CVE: CVE-2018-0843

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. The exploit requires the attacker to have valid credentials to the vulnerable system.

23074 - (MSPT-Feb2018) Microsoft Windows Storage Services Privilege Escalation (CVE-2018-0826)

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

Risk Level: Medium

CVE: CVE-2018-0826

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 Storage Services 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.

23076 - (MSPT-Feb2018) Microsoft Office Out of Bond Memory Error Information Disclosure (CVE-2018-0853)

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

Risk Level: Medium

CVE: CVE-2018-0853

Description

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

Observation

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

The flaw lies in an out of bond memory error. 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.

23080 - (MSPT-Feb2018) Microsoft Windows Font Information Disclosure (CVE-2018-0760)

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

Risk Level: Medium

CVE: CVE-2018-0760

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 Font component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable document.

23081 - (MSPT-Feb2018) Microsoft Windows Font Information Disclosure (CVE-2018-0761)

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

Risk Level: Medium

CVE: CVE-2018-0761

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 Font component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable document.

23082 - (MSPT-Feb2018) Microsoft Windows EOT Font Information Disclosure (CVE-2018-0855)

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

Risk Level: Medium

CVE: CVE-2018-0855

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 EOT Font component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable document.

23091 - (MSPT-Feb2018) Microsoft Windows Kernel Information Disclosure (CVE-2018-0810)

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

Risk Level: Medium

CVE: CVE-2018-0810

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. The exploit requires the user to log on to an affected system and run a specially crafted application.

23092 - (MSPT-Feb2018) Microsoft Windows Kernel Information Disclosure (CVE-2018-0829)

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

Risk Level: Medium

CVE: CVE-2018-0829

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 an attacker could result in the disclosure of sensitive information.

23093 - (MSPT-Feb2018) Microsoft Windows Kernel Information Disclosure (CVE-2018-0830)

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

Risk Level: Medium

CVE: CVE-2018-0830

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 an attacker could result in the disclosure of sensitive information.

23095 - (MSPT-Feb2018) Microsoft Edge Scripting Engine Remote Code Execution (CVE-2018-0836)

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

Risk Level: Medium

CVE: CVE-2018-0836

Description

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

Observation

A vulnerability in some versions of Microsoft 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.

23096 - (MSPT-Feb2018) Microsoft Windows Font Information Disclosure (CVE-2018-0755)

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

Risk Level: Medium

CVE: CVE-2018-0755

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 Font 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.

23098 - (MSPT-Feb2018) Microsoft Windows Kernel Information Disclosure (CVE-2018-0832)

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

Risk Level: Medium

CVE: CVE-2018-0832

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.

23100 - (MSPT-Feb2018) Microsoft Windows Multipoint Privilege Escalation (CVE-2018-0828)

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

Risk Level: Medium

CVE: CVE-2018-0828

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 Multipoint 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.

23102 - (MSPT-Feb2018) Microsoft Windows Scripting Host Security Bypass (CVE-2018-0827)

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

Risk Level: Medium

CVE: CVE-2018-0827

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 Scripting Host component. Successful exploitation by a local attacker could result in the bypass of intended access restrictions.

23106 - (MSPT-Feb2018) Microsoft Edge Request Handling Security Bypass (CVE-2018-0771)

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

Risk Level: Medium

CVE: CVE-2018-0771

Description

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

Observation

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

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

23109 - (MSPT-Feb2018) Microsoft Windows Kernel Information Disclosure (CVE-2018-0757)

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

Risk Level: Medium

CVE: CVE-2018-0757

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.The exploit requires the attacker to have valid credentials to the vulnerable system.

23110 - (MSPT-Feb2018) Microsoft Windows Kernel Privilege Escalation (CVE-2018-0809)

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

Risk Level: Medium

CVE: CVE-2018-0809

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 Kernel component.Successful exploitation could allow a local user to gain elevated privileges.The exploit requires the attacker to have valid credentials to the vulnerable system.

23112 - (MSPT-Feb2018) Microsoft Windows Kernel Privilege Escalation (CVE-2018-0756)

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

Risk Level: Medium

CVE: CVE-2018-0756

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 Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

23113 - (MSPT-Feb2018) Microsoft Windows SMB Denial of Service (CVE-2018-0833)

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

Risk Level: Medium

CVE: CVE-2018-0833

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 SMB component. Successful exploitation by a remote attacker could result in a denial of service condition.

23114 - (MSPT-Feb2018) Microsoft Windows Kernel Privilege Escalation (CVE-2018-0864)

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

Risk Level: Medium

CVE: CVE-2018-0864

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 Kernel component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the attacker to have valid credentials to the vulnerable system.

23115 - (MSPT-Feb2018) Microsoft SharePoint Web Request Sanitization Privilege Escalation (CVE-2018-0869)

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

Risk Level: Medium

CVE: CVE-2018-0869

Description

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

Observation

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

The flaw lies in the Web Request Sanitization 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.

23089 - (MSPT-Feb2018) Microsoft Windows Common Log File System Privilege Escalation (CVE-2018-0844)

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

Risk Level: Informational

CVE: CVE-2018-0844

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 Common Log File System 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.

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.

182586 - FreeBSD clamav Multiple Vulnerabilities (b464f61b-84c7-4e1c-8ad4-6cf9efffd025)

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

Risk Level: High

CVE: CVE-2017-12374, CVE-2017-12375, CVE-2017-12376, CVE-2017-12377, CVE-2017-12378, CVE-2017-12379, CVE-2017-12380

Update Details

Risk is updated

186076 - Ubuntu Linux 14.04, 16.04, 17.10 USN-3550-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12374, CVE-2017-12375, CVE-2017-12376, CVE-2017-12377, CVE-2017-12378, CVE-2017-12379, CVE-2017-12380

Update Details

Risk is updated

130998 - Debian Linux 8.0, 9.0 DSA-4093-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2018-5704

Update Details

Risk is updated

182483 - FreeBSD xorg-server Multiple Vulnabilities (7274e0cc-575f-41bc-8619-14a41b3c2ad0)

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

Risk Level: High

CVE: CVE-2017-12176, CVE-2017-12177, CVE-2017-12178, CVE-2017-12179, CVE-2017-12180, CVE-2017-12181, CVE-2017-12182, CVE-2017-12183, CVE-2017-12184, CVE-2017-12185, CVE-2017-12186, CVE-2017-12187

Update Details

Risk is updated

185916 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3456-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-12176, CVE-2017-12177, CVE-2017-12178, CVE-2017-12179, CVE-2017-12180, CVE-2017-12181, CVE-2017-

12182, CVE-2017-12183, CVE-2017-12184, CVE-2017-12185, CVE-2017-12186, CVE-2017-12187

Update Details

Risk is updated

22998 - (VMSA-2018-0005) VMware Workstation Player Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2017-4949, CVE-2017-4950

Update Details

Risk is updated

23003 - (VMSA-2018-0005) VMware Fusion Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-4949, CVE-2017-4950

Update Details

Risk is updated

88911 - Slackware Linux 14.0, 14.1, 14.2 SSA:2018-024-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000005, CVE-2018-1000007

Update Details

Risk is updated

130995 - Debian Linux 8.0, 9.0 DSA-4087-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5702

Update Details

Risk is updated

131006 - Debian Linux 8.0, 9.0 DSA-4098-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000005, CVE-2018-1000007

Update Details

Risk is updated

182564 - FreeBSD MariaDB Unspecified Vulnerability (b7d89082-e7c0-11e7-ac58-b499baebfeaf)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15365

Update Details
Risk is updated

193202 - Fedora Linux 26 FEDORA-2018-0d6a80f496 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15365

Update Details
Risk is updated

193206 - Fedora Linux 27 FEDORA-2018-d1e263e68e Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-5702

Update Details
Risk is updated

193212 - Fedora Linux 27 FEDORA-2018-241a5a2409 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-1000005, CVE-2018-1000007

Update Details
Risk is updated

193223 - Fedora Linux 26 FEDORA-2018-85655b12b6 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-1000005, CVE-2018-1000007

Update Details
Risk is updated

23046 - Advantech WebAccess Two Vulnerabilities Prior To 8.2.20170817 (ICSA-18-023-01)

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA
Risk Level: Medium
CVE: CVE-2018-5443, CVE-2018-5445

Update Details

Risk is updated

146286 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2018:0217-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000007

Update Details

Risk is updated

146292 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0279-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5748

Update Details

Risk is updated

146297 - SuSE Linux 42.2, 42.3 openSUSE-SU-2018:0236-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-1000007

Update Details

Risk is updated

146307 - SuSE SLES 12 SP3, SLED 12 SP3 SUSE-SU-2018:0295-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6003

Update Details

Risk is updated

146331 - SuSE Linux 42.3 openSUSE-SU-2018:0324-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6003

Update Details

Risk is updated

146348 - SuSE Linux 42.3 openSUSE-SU-2018:0322-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-5748

Update Details

Risk is updated

182575 - FreeBSD unbound Vulnerability In The Processing Of Wildcard Synthesized NSEC Records (8d3bae09-fd28-11e7-95f2-005056925db4)

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

Risk Level: Medium

CVE: CVE-2017-15105

Update Details

Risk is updated

182585 - FreeBSD dovecot Abort Of SASL Authentication Results In A Memory Leak (92b8b284-a3a2-41b1-956c-f9cf8b74f500)

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

Risk Level: Medium

CVE: CVE-2017-15132

Update Details

Risk is updated

182587 - FreeBSD cURL Multiple Vulnerabilities (0cbf0fa6-dcb7-469c-b87a-f94cffd94583)

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

Risk Level: Medium

CVE: CVE-2018-1000007

Update Details

Risk is updated

182590 - FreeBSD W3m - Multiple Vulnerabilities (e72d5bf5-07a0-11e8-8248-0021ccb9e74d)

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

Risk Level: Medium

CVE: CVE-2018-6196, CVE-2018-6197, CVE-2018-6198

Update Details

Risk is updated

193205 - Fedora Linux 27 FEDORA-2018-da4263f065 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2018-6003

Update Details

Risk is updated

193211 - Fedora Linux 27 FEDORA-2018-fbe4017846 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15107

Update Details
Risk is updated

193218 - Fedora Linux 27 FEDORA-2018-69316c5b7a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15105

Update Details
Risk is updated

193234 - Fedora Linux 27 FEDORA-2018-f8c54aeec4 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-6003

Update Details
Risk is updated

193255 - Fedora Linux 26 FEDORA-2018-ef303deec6 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2018-6003

Update Details
Risk is updated

193258 - Fedora Linux 26 FEDORA-2018-9780220f7d Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15107

Update Details
Risk is updated

193261 - Fedora Linux 26 FEDORA-2018-a10a19e06a Update Is Not Installed

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

CVE: CVE-2017-15105

Update Details

Risk is updated

146114 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:3218-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15090, CVE-2017-15092, CVE-2017-15093, CVE-2017-15094

Update Details

Risk is updated

193042 - Fedora Linux 25 FEDORA-2017-81fe39ad9f Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15090, CVE-2017-15092, CVE-2017-15093, CVE-2017-15094

Update Details

Risk is updated

193052 - Fedora Linux 26 FEDORA-2017-1585789772 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15090, CVE-2017-15092, CVE-2017-15093, CVE-2017-15094

Update Details

Risk is updated

193066 - Fedora Linux 27 FEDORA-2017-608b6f5945 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-15090, CVE-2017-15092, CVE-2017-15093, CVE-2017-15094

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

70048 - adobe.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.