2017-NOV-14
FSL version 7.5.974

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

22742 - (APSB17-33) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2017-11213, CVE-2017-11215, CVE-2017-11225, CVE-2017-3112, CVE-2017-3114

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 multiple memory access issues. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

The update provided by Adobe bulletin APSB17-33 resolves the issues. The target system is missing this update.

22743 - (APSB17-33) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-11213, CVE-2017-11215, CVE-2017-11225, CVE-2017-3112, CVE-2017-3114

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 multiple memory access issues. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

The update provided by Adobe bulletin APSB17-33 resolves the issues. The target system is missing this update.

22744 - (APSB17-36) Vulnerabilities In Adobe Reader And Acrobat

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

Risk Level: High

CVE: CVE-2017-11293, CVE-2017-16360, CVE-2017-16361, CVE-2017-16362, CVE-2017-16363, CVE-2017-16364, CVE-2017-16365, CVE-2017-16366, CVE-2017-16367, CVE-2017-16368, CVE-2017-16369, CVE-2017-16370, CVE-2017-16371, CVE-2017-16372, CVE-2017-16373, CVE-2017-16374, CVE-2017-16375, CVE-2017-16376, CVE-2017-16377, CVE-2017-16378, CVE-2017-

16379, CVE-2017-16380, CVE-2017-16381, CVE-2017-16382, CVE-2017-16383, CVE-2017-16384, CVE-2017-16385, CVE-2017-16386, CVE-2017-16387, CVE-2017-16388, CVE-2017-16389, CVE-2017-16390, CVE-2017-16391, CVE-2017-16392, CVE-2017-16393, CVE-2017-16394, CVE-2017-16395, CVE-2017-16396, CVE-2017-16397, CVE-2017-16398, CVE-2017-16399, CVE-2017-16400, CVE-2017-16401, CVE-2017-16402, CVE-2017-16403, CVE-2017-16404, CVE-2017-16405, CVE-2017-16406, CVE-2017-16407, CVE-2017-16408, CVE-2017-16409, CVE-2017-16410, CVE-2017-16411, CVE-2017-16412, CVE-2017-16413, CVE-2017-16414, CVE-2017-16415, CVE-2017-16416, CVE-2017-16417, CVE-2017-16418, CVE-2017-16419, CVE-2017-16420

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 remotely execute arbitrary code or disclose sensitive information.

The update provided by Adobe bulletin APSB17-36 resolves these issues. The target system appears to be missing this update.

22675 - (MSPT-Nov2017) Microsoft Office Excel Remote Code Execution (CVE-2017-11878)

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

Risk Level: High

CVE: CVE-2017-11878

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 Excel 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.

22676 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-11836)

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

Risk Level: High

CVE: CVE-2017-11836

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 in Microsoft Edge. 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.

22677 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-11862)

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

Risk Level: High

CVE: CVE-2017-11862

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 in Microsoft Edge. 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.

22678 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-11870)

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

Risk Level: High

CVE: CVE-2017-11870

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 in Microsoft Edge. 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.

22679 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-11873)

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

Risk Level: High

CVE: CVE-2017-11873

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 in Microsoft Edge. 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.

22686 - (MSPT-Nov2017) Microsoft Internet Explorer Memory Handling Remote Code Execution (CVE-2017-11855)

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

Risk Level: High

CVE: CVE-2017-11855

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 Memory Handling 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.

22687 - (MSPT-Nov2017) Microsoft Internet Explorer Memory Handling Remote Code Execution (CVE-2017-11856)

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

Risk Level: High

CVE: CVE-2017-11856

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 Memory Handling 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.

22688 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-11869)

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

Risk Level: High

CVE: CVE-2017-11869

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.

22691 - (MSPT-Nov2017) Microsoft Office Word Remote Code Execution (CVE-2017-11854)

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

Risk Level: High

CVE: CVE-2017-11854

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 Word 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.

22696 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-11840)

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

Risk Level: High

CVE: CVE-2017-11840

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.

22698 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-11871)

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

Risk Level: High

CVE: CVE-2017-11871

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.

22702 - (MSPT-Nov2017) Windows Kernel Elevation Of Privilege Vulnerability (CVE-2017-11847)

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

Risk Level: High

CVE: CVE-2017-11847

Description

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

Observation

Windows is a popular operating 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 handles objects in memory. Successful exploitation could allow an attacker to violate virtual trust levels. Exploitation requires an attacker to gain access to the local system.

22715 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Memory Corruption Vulnerability (CVE-2017-11837)

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

Risk Level: High

CVE: CVE-2017-11837

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.

22716 - (MSPT-Nov2017) Microsoft Browser Memory Corruption Vulnerability (CVE-2017-11827)

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

Risk Level: High

CVE: CVE-2017-11827

Description

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

Observation

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

The flaw lies in how Microsoft browsers access 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.

22717 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Memory Corruption Vulnerability (CVE-2017-11838)

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

Risk Level: High

CVE: CVE-2017-11838

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 how the scripting engine 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.

22718 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Memory Corruption Vulnerability (CVE-2017-11843)

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

Risk Level: High

CVE: CVE-2017-11843

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 how the scripting engine 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.

22719 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Memory Corruption Vulnerability (CVE-2017-11846)

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

Risk Level: High

CVE: CVE-2017-11846

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 how the scripting engine 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.

22720 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Memory Corruption Vulnerability (CVE-2017-11858)

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

Risk Level: High

CVE: CVE-2017-11858

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 how Microsoft browsers access 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.

22726 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-11866)

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

Risk Level: High

CVE: CVE-2017-11866

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.

22727 - (MSPT-Nov2017) Microsoft Office Memory Handling Remote Code Execution (CVE-2017-11882)

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

Risk Level: High

CVE: CVE-2017-11882

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 Memory Handling 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.

22683 - (MSPT-Nov2017) Microsoft Windows Search Denial of Service (CVE-2017-11788)

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

Risk Level: Medium

CVE: CVE-2017-11788

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

22673 - (MSPT-Nov2017) Microsoft Office Project Privilege Escalation (CVE-2017-11876)

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

Risk Level: Medium

CVE: CVE-2017-11876

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 Project 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.

22674 - (MSPT-Nov2017) Microsoft Office Excel Security Bypass (CVE-2017-11877)

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

Risk Level: Medium

CVE: CVE-2017-11877

Description

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

Observation

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

The flaw lies in the Excel 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.

22680 - (MSPT-Nov2017) Microsoft Edge Edge Security Bypass (CVE-2017-11863)

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

Risk Level: Medium

CVE: CVE-2017-11863

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 validation of Edge Content Security Policy (CSP). 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.

22681 - (MSPT-Nov2017) Microsoft Edge Security Feature Bypass Vulnerability (CVE-2017-11872)

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

Risk Level: Medium

CVE: CVE-2017-11872

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 is due to improper handling of redirect requests. Successful exploitation by a remote attacker could result in the bypass of Cross-Origin Resource Sharing (CORS) redirect restrictions. The exploit requires the user to open a vulnerable website, email or document.

22682 - (MSPT-Nov2017) Microsoft Edge Security Feature Bypass Vulnerability (CVE-2017-11874)

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

Risk Level: Medium

CVE: CVE-2017-11874

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 way memory is accessed in code compiled by the Edge Just-In-Time (JIT) compiler. Successful exploitation by a remote attacker could result in the bypass of Control Flow Guard (CFG) access restrictions. The exploit requires the user to open a vulnerable website, email or document.

22684 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Information Disclosure (CVE-2017-11834)

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

Risk Level: Medium

CVE: CVE-2017-11834

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 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.

22685 - (MSPT-Nov2017) Microsoft Internet Explorer Page Content Information Disclosure (CVE-2017-11848)

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

Risk Level: Medium

CVE: CVE-2017-11848

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 lies in the Page Content 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.

22692 - (MSPT-Nov2017) Microsoft Windows Graphics Information Disclosure (CVE-2017-11850)

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

Risk Level: Medium

CVE: CVE-2017-11850

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 user to open a vulnerable website, email or document.

22693 - (MSPT-Nov2017) Microsoft Windows Font Engine Information Disclosure (CVE-2017-11832)

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

Risk Level: Medium

CVE: CVE-2017-11832

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 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.

22694 - (MSPT-Nov2017) Microsoft Windows Font Engine Information Disclosure (CVE-2017-11835)

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

Risk Level: Medium

CVE: CVE-2017-11835

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 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.

22695 - (MSPT-Nov2017) Microsoft Windows Media Player Information Disclosure (CVE-2017-11768)

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

Risk Level: Medium

CVE: CVE-2017-11768

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 Media Player 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.

22706 - (MSPT-Nov2017) Microsoft Edge Memory Handling Information Disclosure (CVE-2017-11803)

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

Risk Level: Medium

CVE: CVE-2017-11803

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 Memory Handling 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.

22707 - (MSPT-Nov2017) Microsoft Edge Cross Origin Request Information Disclosure (CVE-2017-11833)

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

Risk Level: Medium

CVE: CVE-2017-11833

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 Cross Origin Request 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.

22708 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-11839)

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

Risk Level: Medium

CVE: CVE-2017-11839

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.

22709 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-11841)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-11841

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.

22710 - (MSPT-Nov2017) Microsoft Edge Memory Handling Information Disclosure (CVE-2017-11844)

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

Risk Level: Medium

CVE: CVE-2017-11844

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 Memory Handling 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.

22711 - (MSPT-Nov2017) Microsoft Edge Memory Handling Remote Code Execution (CVE-2017-11845)

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

Risk Level: Medium

CVE: CVE-2017-11845

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 Memory Handling 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.

22712 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Remote Code Execution (CVE-2017-11861)

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

Risk Level: Medium

CVE: CVE-2017-11861

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.

22714 - (MSPT-Nov2017) Microsoft Windows Scripting Engine Information Disclosure (CVE-2017-11791)

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

Risk Level: Medium

CVE: CVE-2017-11791

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 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.

22724 - (MSPT-Nov2017) Microsoft Windows GDI Information Disclosure (CVE-2017-11852)

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

Risk Level: Medium

CVE: CVE-2017-11852

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 open a vulnerable website, email or document.

22725 - (MSPT-Nov2017) Microsoft Windows Device Guard Security Bypass (CVE-2017-11830)

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

Risk Level: Medium

CVE: CVE-2017-11830

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 user to open a vulnerable website, email or document.

22737 - (MSPT-Nov2017) Microsoft Office Excel Security Bypass (CVE-2017-11877)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-11877

Description

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

Observation

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

The flaw lies in the Excel 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.

22699 - (MSPT-Nov2017) Windows Information Disclosure Vulnerability (CVE-2017-11831)

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

Risk Level: Low

CVE: CVE-2017-11831

Description

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

Observation

Windows is a popular operating system developed by Microsoft.

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

22700 - (MSPT-Nov2017) Windows Kernel Information Disclosure Vulnerability (CVE-2017-11851)

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

Risk Level: Low

CVE: CVE-2017-11851

Description

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

Observation

Windows is a popular operating 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.

22701 - (MSPT-Nov2017) Windows Kernel Information Disclosure Vulnerability (CVE-2017-11842)

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

Risk Level: Low

CVE: CVE-2017-11842

Description

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

Observation

Windows is a popular operating system developed by Microsoft.

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

22703 - (MSPT-Nov2017) Windows Kernel Information Disclosure Vulnerability (CVE-2017-11849)

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

Risk Level: Low

CVE: CVE-2017-11849

Description

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

Observation

Windows is a popular operating system developed by Microsoft.

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

22704 - (MSPT-Nov2017) Windows Kernel Information Disclosure Vulnerability (CVE-2017-11853)

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

Risk Level: Low

CVE: CVE-2017-11853

Description

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

Observation

Windows is a popular operating system developed by Microsoft.

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

22705 - (MSPT-Nov2017) Windows Information Disclosure Vulnerability (CVE-2017-11880)

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

Risk Level: Low

CVE: CVE-2017-11880

Description

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

Observation

Windows is a popular operating system developed by Microsoft.

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

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.

145851 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:0909-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056

Update Details

Risk is updated

178421 - Gentoo Linux GLSA-201704-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056

Update Details

Risk is updated

182318 - FreeBSD chromium Multiple Vulnerabilities (7cf058d8-158d-11e7-ba2c-e8e0b747a45a)

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

Risk Level: High

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056

Update Details

Risk is updated

191912 - Fedora Linux 25 FEDORA-2017-ff6940bf63 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056

Update Details

Risk is updated

191950 - Fedora Linux 26 FEDORA-2017-49f828d4b1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056

Update Details

Risk is updated

192160 - Fedora Linux 24 FEDORA-2017-7d698eba8b Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-5052, CVE-2017-5053, CVE-2017-5054, CVE-2017-5055, CVE-2017-5056, CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5068, CVE-2017-5069

Update Details

Risk is updated

170565 - Amazon Linux AMI ALAS-2015-588 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5739, CVE-2015-5740, CVE-2015-5741

Update Details

Risk is updated

181569 - FreeBSD go Multiple Vulnerabilities (4464212e-4acd-11e5-934b-002590263bf5)

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

Risk Level: High

CVE: CVE-2015-5739, CVE-2015-5740, CVE-2015-5741

Update Details

Risk is updated

189636 - Fedora Linux 21 FEDORA-2015-12957 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5739, CVE-2015-5740, CVE-2015-5741

Update Details

Risk is updated

189653 - Fedora Linux 22 FEDORA-2015-13002 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5739, CVE-2015-5740, CVE-2015-5741

Update Details

Risk is updated

189796 - Fedora Linux 22 FEDORA-2015-15619 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5739, CVE-2015-5740, CVE-2015-5741

Update Details

Risk is updated

189797 - Fedora Linux 21 FEDORA-2015-15618 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-5739, CVE-2015-5740, CVE-2015-5741

Update Details

Risk is updated

192838 - Fedora Linux 25 FEDORA-2017-ebab38baf6 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15951

Update Details

Risk is updated

192861 - Fedora Linux 26 FEDORA-2017-10faeda281 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-15951

Update Details

Risk is updated

21684 - Google Chrome Multiple Vulnerabilities Prior To 58.0.3029.81

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

Risk Level: Medium

CVE: CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5069

Update Details

Risk is updated

21685 - Google Chrome Multiple Vulnerabilities Prior To 58.0.3029.81

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5069

Update Details

Risk is updated

21910 - Google Chrome Multiple Vulnerabilities Prior To 59.0.3071.86

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

Risk Level: Medium

CVE: CVE-2017-5070, CVE-2017-5071, CVE-2017-5072, CVE-2017-5073, CVE-2017-5074, CVE-2017-5075, CVE-2017-5076, CVE-2017-5077, CVE-2017-5078, CVE-2017-5079, CVE-2017-5080, CVE-2017-5081, CVE-2017-5082, CVE-2017-5083, CVE-2017-5085, CVE-2017-5086

Update Details

Risk is updated

21911 - Google Chrome Multiple Vulnerabilities Prior To 59.0.3071.86

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-5070, CVE-2017-5071, CVE-2017-5072, CVE-2017-5073, CVE-2017-5074, CVE-2017-5075, CVE-2017-5076, CVE-2017-5077, CVE-2017-5078, CVE-2017-5079, CVE-2017-5080, CVE-2017-5081, CVE-2017-5082, CVE-2017-5083, CVE-2017-5085, CVE-2017-5086

Update Details

Risk is updated

22010 - Google Chrome Multiple Vulnerabilities Prior To 59.0.3071.104

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

Risk Level: Medium

CVE: CVE-2017-5087, CVE-2017-5088, CVE-2017-5089

Update Details

Risk is updated

22011 - Google Chrome Multiple Vulnerabilities Prior To 59.0.3071.104

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-5087, CVE-2017-5088, CVE-2017-5089

Update Details

Risk is updated

22456 - Google Chrome Multiple Vulnerabilities Prior To 61.0.3163.79

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

Risk Level: Medium

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120

Update Details

Risk is updated

22457 - Google Chrome Multiple Vulnerabilities Prior To 61.0.3163.79

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120

Update Details

Risk is updated

130834 - Debian Linux 9.0 DSA-3926-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5087, CVE-2017-5088, CVE-2017-5089, CVE-2017-5091, CVE-2017-5092, CVE-2017-5093, CVE-2017-5094, CVE-2017-5095, CVE-2017-5097, CVE-2017-5098, CVE-2017-5099, CVE-2017-5100, CVE-2017-5101, CVE-2017-5102, CVE-2017-5103, CVE-2017-5104, CVE-2017-5105, CVE-2017-5106, CVE-2017-5107, CVE-2017-5108, CVE-2017-5109, CVE-2017-5110, CVE-2017-7000

Update Details

Risk is updated

130894 - Debian Linux 9.0 DSA-3985-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120, CVE-2017-5121, CVE-2017-5122

Update Details

Risk is updated

141550 - Red Hat Enterprise Linux RHSA-2017-1124 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5069

Update Details

Risk is updated

141595 - Red Hat Enterprise Linux RHSA-2017-1495 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5087, CVE-2017-5088, CVE-2017-5089

Update Details

Risk is updated

141609 - Red Hat Enterprise Linux RHSA-2017-1399 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5070, CVE-2017-5071, CVE-2017-5072, CVE-2017-5073, CVE-2017-5074, CVE-2017-5075, CVE-2017-5076, CVE-2017-5077, CVE-2017-5078, CVE-2017-5079, CVE-2017-5080, CVE-2017-5081, CVE-2017-5082, CVE-2017-5083, CVE-2017-5085, CVE-2017-5086

Update Details

Risk is updated

141712 - Red Hat Enterprise Linux RHSA-2017-2676 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120

Update Details

Risk is updated

145621 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1098-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5069

Update Details

Risk is updated

145757 - SuSE Linux 42.2 openSUSE-SU-2017:1502-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5070, CVE-2017-5071, CVE-2017-5072, CVE-2017-5073, CVE-2017-5074, CVE-2017-5075, CVE-2017-5076, CVE-2017-5077, CVE-2017-5078, CVE-2017-5079, CVE-2017-5080, CVE-2017-5081, CVE-2017-5082, CVE-2017-5083, CVE-2017-5085, CVE-2017-5086

Update Details

Risk is updated

145859 - SuSE Linux 42.2 openSUSE-SU-2017:1591-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5087, CVE-2017-5088, CVE-2017-5089

Update Details

Risk is updated

145923 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2491-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120

Update Details

Risk is updated

178425 - Gentoo Linux GLSA-201705-02 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5069

Update Details

Risk is updated

178455 - Gentoo Linux GLSA-201706-20 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5068, CVE-2017-5070, CVE-2017-5071, CVE-2017-5072, CVE-2017-5073, CVE-2017-5074, CVE-2017-5075, CVE-2017-5076, CVE-2017-5077, CVE-2017-5078, CVE-2017-5079, CVE-2017-5080, CVE-2017-5081, CVE-2017-5082, CVE-2017-5083, CVE-2017-5084, CVE-2017-5085, CVE-2017-5086, CVE-2017-5087, CVE-2017-5088, CVE-2017-5089

Update Details

Risk is updated

182332 - FreeBSD chromium Multiple Vulnerabilities (95a74a48-2691-11e7-9e2d-e8e0b747a45a)

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

Risk Level: Medium

CVE: CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5069

Update Details

Risk is updated

182364 - FreeBSD chromium Multiple Vulnerabilities (52f4b48b-4ac3-11e7-99aa-e8e0b747a45a)

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

Risk Level: Medium

CVE: CVE-2017-5070, CVE-2017-5071, CVE-2017-5072, CVE-2017-5073, CVE-2017-5074, CVE-2017-5075, CVE-2017-5076, CVE-2017-5077, CVE-2017-5078, CVE-2017-5079, CVE-2017-5080, CVE-2017-5081, CVE-2017-5082, CVE-2017-5083, CVE-2017-5085, CVE-2017-5086

Update Details

Risk is updated

182375 - FreeBSD chromium Multiple Vulnerabilities (f53dd5cc-527f-11e7-a772-e8e0b747a45a)

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

Risk Level: Medium

CVE: CVE-2017-5087, CVE-2017-5088, CVE-2017-5089

Update Details

Risk is updated

182437 - FreeBSD chromium Multiple Vulnerabilities (e1100e63-92f7-11e7-bd95-e8e0b747a45a)

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

Risk Level: Medium

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120

Update Details

Risk is updated

192131 - Fedora Linux 25 FEDORA-2017-dc7ce3b314 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5068, CVE-2017-5069

Update Details

Risk is updated

192218 - Fedora Linux 26 FEDORA-2017-811133dc2c Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5057, CVE-2017-5058, CVE-2017-5059, CVE-2017-5060, CVE-2017-5061, CVE-2017-5062, CVE-2017-5063, CVE-2017-5064, CVE-2017-5065, CVE-2017-5066, CVE-2017-5067, CVE-2017-5068, CVE-2017-5069

Update Details

Risk is updated

192266 - Fedora Linux 24 FEDORA-2017-c2e1dc46a1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5087, CVE-2017-5088, CVE-2017-5089

Update Details

Risk is updated

192276 - Fedora Linux 26 FEDORA-2017-c11d7ef69a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5070, CVE-2017-5071, CVE-2017-5072, CVE-2017-5073, CVE-2017-5074, CVE-2017-5075, CVE-2017-5076, CVE-2017-5077, CVE-2017-5078, CVE-2017-5079, CVE-2017-5080, CVE-2017-5081, CVE-2017-5082, CVE-2017-5083, CVE-2017-5085, CVE-2017-5086

Update Details

Risk is updated

192281 - Fedora Linux 26 FEDORA-2017-01e4d46f23 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5087, CVE-2017-5088, CVE-2017-5089

Update Details

Risk is updated

192291 - Fedora Linux 25 FEDORA-2017-e8a1e1e62a Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5087, CVE-2017-5088, CVE-2017-5089

Update Details

Risk is updated

192302 - Fedora Linux 25 FEDORA-2017-a66e2c5b62 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5070, CVE-2017-5071, CVE-2017-5072, CVE-2017-5073, CVE-2017-5074, CVE-2017-5075, CVE-2017-5076, CVE-2017-5077, CVE-2017-5078, CVE-2017-5079, CVE-2017-5080, CVE-2017-5081, CVE-2017-5082, CVE-2017-5083, CVE-2017-5085, CVE-2017-5086

Update Details

Risk is updated

192338 - Fedora Linux 24 FEDORA-2017-b8d76bef4e Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5070, CVE-2017-5071, CVE-2017-5072, CVE-2017-5073, CVE-2017-5074, CVE-2017-5075, CVE-2017-5076, CVE-2017-5077, CVE-2017-5078, CVE-2017-5079, CVE-2017-5080, CVE-2017-5081, CVE-2017-5082, CVE-2017-5083, CVE-2017-5085, CVE-2017-5086

Update Details

Risk is updated

192387 - Fedora Linux 26 FEDORA-2017-1e34da27f3 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5070, CVE-2017-5071, CVE-2017-5075, CVE-2017-5076, CVE-2017-5077, CVE-2017-5078, CVE-2017-5079, CVE-2017-5083, CVE-2017-5088, CVE-2017-5089

Update Details

Risk is updated

192391 - Fedora Linux 25 FEDORA-2017-a7a488d8d0 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5070, CVE-2017-5071, CVE-2017-5075, CVE-2017-5076, CVE-2017-5077, CVE-2017-5078, CVE-2017-5079, CVE-2017-5083, CVE-2017-5088, CVE-2017-5089

Update Details

Risk is updated

192493 - Fedora Linux 24 FEDORA-2017-5b199bf121 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5052, CVE-2017-5054

Update Details

Risk is updated

192700 - Fedora Linux 27 FEDORA-2017-109f8db088 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120, CVE-2017-5121, CVE-2017-5122

Update Details

Risk is updated

192791 - Fedora Linux 26 FEDORA-2017-efeb59171d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5111, CVE-2017-5112, CVE-2017-5113, CVE-2017-5114, CVE-2017-5115, CVE-2017-5116, CVE-2017-5117, CVE-2017-5118, CVE-2017-5119, CVE-2017-5120, CVE-2017-5121, CVE-2017-5122

Update Details

Risk is updated

130806 - Debian Linux 8.0 DSA-3897-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-7943, CVE-2017-6922

Update Details

Risk is updated

141572 - Red Hat Enterprise Linux RHSA-2017-1228 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Red Hat Enterprise Linux Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2017-5068

Update Details

Risk is updated

145763 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1190-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-5068

Update Details

Risk is updated

181655 - FreeBSD drupal Open Redirect Vulnerability (75f39413-7a00-11e5-a2a1-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-7943

Update Details

Risk is updated

182345 - FreeBSD chromium Race Condition Vulnerability (92e345d0-304d-11e7-8359-e8e0b747a45a)

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

Risk Level: Medium

CVE: CVE-2017-5068

Update Details

Risk is updated

185944 - Ubuntu Linux 17.04, 17.10 USN-3466-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-15908

Update Details
Risk is updated

188437 - Fedora Linux 21 FEDORA-2014-14283 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-8321, CVE-2014-8322, CVE-2014-8323, CVE-2014-8324

Update Details
Risk is updated

188507 - Fedora Linux 20 FEDORA-2014-14247 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-8321, CVE-2014-8322, CVE-2014-8323, CVE-2014-8324

Update Details
Risk is updated

188512 - Fedora Linux 19 FEDORA-2014-14233 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2014-8321, CVE-2014-8322, CVE-2014-8323, CVE-2014-8324

Update Details
Risk is updated

189888 - Fedora Linux 23 FEDORA-2015-ccf2b449a9 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-7943

Update Details
Risk is updated

189950 - Fedora Linux 22 FEDORA-2015-cb94fd13d8 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-7943

Update Details
Risk is updated

189402 - Fedora Linux 22 FEDORA-2015-8684 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2156

Update Details

Risk is updated

189408 - Fedora Linux 21 FEDORA-2015-8713 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-2156

Update Details

Risk is updated

192847 - Fedora Linux 26 FEDORA-2017-a47c76eeb1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15096

Update Details

Risk is updated

192862 - Fedora Linux 25 FEDORA-2017-150762f6be Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-15096

Update Details

Risk 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.