2017-OCT-10
FSL version 7.5.965

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

22533 - (MSPT-Oct2017) Microsoft Windows DNSAPI Remote Code Execution (CVE-2017-11779)

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

Risk Level: High

CVE: CVE-2017-11779

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 DNSAPI 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.

22536 - (MSPT-Oct2017) Microsoft Windows Graphics Remote Code Execution (CVE-2017-11762)

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

Risk Level: High

CVE: CVE-2017-11762

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 Graphics 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.

22537 - (MSPT-Oct2017) Microsoft Windows Graphics Remote Code Execution (CVE-2017-11763)

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

Risk Level: High

CVE: CVE-2017-11763

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 Graphics 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.

22539 - (MSPT-Oct2017) Microsoft Windows Search Remote Code Execution (CVE-2017-11771)

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

Risk Level: High

CVE: CVE-2017-11771

Description

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

Observation

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

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

22549 - (MSPT-Oct2017) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2017-11793)

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

Risk Level: High

CVE: CVE-2017-11793

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.

22550 - (MSPT-Oct2017) Microsoft Internet Explorer Scripting Engine Remote Code Execution (CVE-2017-11810)

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

Risk Level: High

CVE: CVE-2017-11810

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.

22551 - (MSPT-Oct2017) Microsoft Internet Explorer Memory Corruption Remote Code Execution (CVE-2017-11813)

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

Risk Level: High

CVE: CVE-2017-11813

Description

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

Observation

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

The flaw is due to improper accesses of 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.

22552 - (MSPT-Oct2017) Microsoft Internet Explorer Memory Corruption Remote Code Execution (CVE-2017-11822)

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

Risk Level: High

CVE: CVE-2017-11822

Description

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

Observation

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

The flaw is due to improper handling of 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.

22553 - (MSPT-Oct2017) Microsoft Internet Explorer Memory Corruption Remote Code Execution (CVE-2017-8727)

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

Risk Level: High

CVE: CVE-2017-8727

Description

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

Observation

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

The flaw is due to improper accesses of 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.

22554 - (MSPT-Oct2017) Microsoft Windows Browsers Remote Code Execution (CVE-2017-11819)

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

Risk Level: High

CVE: CVE-2017-11819

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 Browsers 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.

22508 - (MSPT-Oct2017) Microsoft Windows JET Database Remote Code Execution (CVE-2017-8717)

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

Risk Level: High

CVE: CVE-2017-8717

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 JET Database 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.

22509 - (MSPT-Oct2017) Microsoft Windows JET Database Remote Code Execution (CVE-2017-8718)

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

Risk Level: High

CVE: CVE-2017-8718

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 JET Database 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.

22510 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11792)

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

Risk Level: High

CVE: CVE-2017-11792

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22511 - (MSPT-Oct2017) Microsoft Edge Information Disclosure Vulnerability (CVE-2017-11794)

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

Risk Level: High

CVE: CVE-2017-11794

Description

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

Observation

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

An information disclosure vulnerability is present in some versions of Microsoft Edge. The flaw lies in how the Microsoft Edge handles objects in memory. Successful exploitation could allow an attacker to obtain restricted information.

22512 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11796)

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

Risk Level: High

CVE: CVE-2017-11796

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22513 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11798)

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

Risk Level: High

CVE: CVE-2017-11798

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

A remote code execution vulnerability is present in some versions of Microsoft Edge. The flaw lies in how the Scripting Engine handles

objects in memory. Successful exploitation could allow an attacker to remotely execute arbitrary code on the target system.

22514 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11799)

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

Risk Level: High

CVE: CVE-2017-11799

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22515 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11800)

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

Risk Level: High

CVE: CVE-2017-11800

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22516 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11802)

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

Risk Level: High

CVE: CVE-2017-11802

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22518 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11804)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2017-11804

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22519 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11805)

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

Risk Level: High

CVE: CVE-2017-11805

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22520 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11806)

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

Risk Level: High

CVE: CVE-2017-11806

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22521 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11807)

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

Risk Level: High

CVE: CVE-2017-11807

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22522 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11808)

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

Risk Level: High

CVE: CVE-2017-11808

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22523 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11809)

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

Risk Level: High

CVE: CVE-2017-11809

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22524 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11811)

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

Risk Level: High

CVE: CVE-2017-11811

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22525 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11812)

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

Risk Level: High

CVE: CVE-2017-11812

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22526 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-11821)

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

Risk Level: High

CVE: CVE-2017-11821

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22527 - (MSPT-Oct2017) Microsoft Edge Scripting Engine Memory Corruption Vulnerability (CVE-2017-8726)

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

Risk Level: High

CVE: CVE-2017-8726

Description

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

Observation

Microsoft Edge is the Windows 10 browser by default.

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

22545 - (MSPT-Oct2017) Microsoft Windows TRIE Remote Code Execution (CVE-2017-11769)

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

Risk Level: High

CVE: CVE-2017-11769

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 TRIE 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.

22548 - (MSPT-Oct2017) Microsoft Internet Explorer Memory Corruption Information Disclosure (CVE-2017-11790)

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

Risk Level: High

CVE: CVE-2017-11790

Description

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

Observation

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

The flaw is due to improper handling of objects in memory. 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.

22555 - (MSPT-Oct2017) Microsoft Windows Advanced Local Procedure Call Privilege Escalation (CVE-2017-11783)

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

Risk Level: High

CVE: CVE-2017-11783

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 Advanced Local procedure Call 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.

22558 - (MSPT-Oct2017) Microsoft Windows Kernel-Mode Driver Privilege Escalation (CVE-2017-8689)

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

Risk Level: High

CVE: CVE-2017-8689

Description

An elevation of privilege vulnerability in some versions of Microsoft Windows could lead to code execution in kernel mode.

Observation

An elevation of privilege vulnerability in some versions of Microsoft Windows could lead to code execution in kernel mode.

The flaw lies in the Windows kernel-mode driver. Successful exploitation could allow a local user to gain elevated privileges.The exploit requires the attacker to have valid credentials to the vulnerable system.

22559 - (MSPT-Oct2017) Microsoft Windows Kernel -Mode Driver Privilege Escalation (CVE-2017-8694)

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

Risk Level: High

CVE: CVE-2017-8694

Description

An elevation of privilege vulnerability in some versions of Microsoft Windows could lead to code execution in kernel mode.

Observation

An elevation of privilege vulnerability in some versions of Microsoft Windows could lead to code execution in kernel mode.

The flaw lies in the Windows kernel-mode driver. Successful exploitation could allow a local user to gain elevated privileges.The exploit requires the attacker to have valid credentials to the vulnerable system.

22569 - (MSPT-Oct2017) Microsoft Windows Subsystem for Linux Denial of Service (CVE-2017-8703)

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

Risk Level: High

CVE: CVE-2017-8703

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

22587 - (MSPT-Oct2017) Microsoft Office Memory Corruption Vulnerability (CVE-2017-11826)

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

Risk Level: High

CVE: CVE-2017-11826

Description

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

Observation

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

The flaw is due to improper handling of objects. 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.

22530 - (MSPT-Oct2017) Microsoft Office Sharepoint Privilege Escalation (CVE-2017-11775)

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

Risk Level: Medium

CVE: CVE-2017-11775

Description

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

Observation

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

The flaw lies in the SharePoint component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

22531 - (MSPT-Oct2017) Microsoft Office Sharepoint Privilege Escalation (CVE-2017-11777)

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

Risk Level: Medium

CVE: CVE-2017-11777

Description

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

Observation

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

The flaw lies in the SharePoint component. Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

22532 - (MSPT-Oct2017) Microsoft Office Sharepoint Privilege Escalation (CVE-2017-11820)

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

Risk Level: Medium

CVE: CVE-2017-11820

Description

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

Observation

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

The flaw lies in the Sharepoint component.Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

22534 - (MSPT-Oct2017) Microsoft Windows GDI Information Disclosure (CVE-2017-11816)

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

Risk Level: Medium

CVE: CVE-2017-11816

Description

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

Observation

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

The flaw lies in the GDI component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

22535 - (MSPT-Oct2017) Microsoft Windows Graphics Information Disclosure (CVE-2017-8693)

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

Risk Level: Medium

CVE: CVE-2017-8693

Description

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

Observation

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

The flaw lies in the Graphics component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

22538 - (MSPT-Oct2017) Microsoft Windows Graphics Privilege Escalation (CVE-2017-11824)

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

Risk Level: Medium

CVE: CVE-2017-11824

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 Graphics 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.

22540 - (MSPT-Oct2017) Microsoft Windows Search Information Disclosure (CVE-2017-11772)

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

Risk Level: Medium

CVE: CVE-2017-11772

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 Search 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.

22541 - (MSPT-Oct2017) Microsoft Windows SMB Remote Code Execution (CVE-2017-11780)

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

Risk Level: Medium

CVE: CVE-2017-11780

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 SMB 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.

22542 - (MSPT-Oct2017) Microsoft Windows SMB Information Disclosure (CVE-2017-11815)

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

Risk Level: Medium

CVE: CVE-2017-11815

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 SMB 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.

22543 - (MSPT-Oct2017) Microsoft Windows SMB Denial of Service (CVE-2017-11781)

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

Risk Level: Medium

CVE: CVE-2017-11781

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. The exploit requires the user to open a vulnerable website, email or document.

22544 - (MSPT-Oct2017) Microsoft Windows SMB Privilege Escalation (CVE-2017-11782)

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

Risk Level: Medium

CVE: CVE-2017-11782

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 SMB 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.

22560 - (MSPT-Oct2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-11765)

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

Risk Level: Medium

CVE: CVE-2017-11765

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 local attacker could result in the disclosure of sensitive information.The exploit requires the attacker to have valid credentials to the vulnerable system.

22561 - (MSPT-Oct2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-11784)

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

Risk Level: Medium

CVE: CVE-2017-11784

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 local attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

22562 - (MSPT-Oct2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-11785)

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

Risk Level: Medium

CVE: CVE-2017-11785

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 local attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

22563 - (MSPT-Oct2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-11814)

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

Risk Level: Medium

CVE: CVE-2017-11814

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 local attacker could result in the disclosure of sensitive information.The exploit requires the attacker to have valid credentials to the vulnerable system.

22564 - (MSPT-Oct2017) Microsoft Windows Kernel Information Disclosure (CVE-2017-11817)

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

Risk Level: Medium

CVE: CVE-2017-11817

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 local attacker could result in the disclosure of sensitive information. The exploit requires the attacker to have valid credentials to the vulnerable system.

22568 - (MSPT-Oct2017) Microsoft Windows Storage Security Bypass (CVE-2017-11818)

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

Risk Level: Medium

CVE: CVE-2017-11818

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 Storage 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.

22570 - (MSPT-Oct2017) Microsoft Windows Device Guard Security Bypass (CVE-2017-8715)

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

Risk Level: Medium

CVE: CVE-2017-8715

Description

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

Observation

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

The flaw lies in the Device Guard component. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. The exploit requires the attacker to have valid credentials to the vulnerable system.

22571 - (MSPT-Oct2017) Microsoft Windows Device Guard Security Bypass (CVE-2017-11823)

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

Risk Level: Medium

CVE: CVE-2017-11823

Description

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

Observation

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

The flaw lies in the Device Guard component. Successful exploitation by a remote attacker could result in the bypass of intended access restrictions. The exploit requires the attacker to have valid credentials to the vulnerable system.

22572 - (MSPT-Oct2017) Microsoft Office Outlook Security Bypass (CVE-2017-11774)

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

Risk Level: Medium

CVE: CVE-2017-11774

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 Outlook 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.

22573 - (MSPT-Oct2017) Microsoft Office Outlook Information Disclosure (CVE-2017-11776)

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

Risk Level: Medium

CVE: CVE-2017-11776

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 the Outlook 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.

22574 - (MSPT-Oct2017) Microsoft Office Memory Corruption Remote Code Execution (CVE-2017-11825)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-11825

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 how this software 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.

22577 - (MSPT-Oct2017) Microsoft Office Skype for Business Elevation of Privilege Vulnerability (CVE-2017-11786)

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

Risk Level: Medium

CVE: CVE-2017-11786

Description

A vulnerability in some versions of Microsoft Skype for Business could lead to elevation of privileges.

Observation

A vulnerability in some versions of Microsoft Skype for Business could lead to elevation of privileges.

The flaw is due to a failure in handling handle specific authentication requests in Skype for Business.The exploit requires attacker to invite a user to an instant message session while using a malicious profile image. Successful exploitation by an attacker could result in

elevation of privileges.

22591 - (MSPT-Oct2017) Microsoft Windows Update Delivery Privilege Escalation (CVE-2017-11829)

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

Risk Level: Medium

CVE: CVE-2017-11829

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 Update Delivery 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.

22578 - (MSPT-Oct2017) Vulnerability in TPM could allow Security Feature Bypass (ADV170012)

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

Risk Level: Low

CVE: CVE-MAP-NOMATCH

Description

A vulnerability in some vendor's TPM chipset firmware could allow security feature bypass.

Observation

A vulnerability in some vendor's TPM chipset firmware could allow security feature bypass.

The flaw is due to a failure in third party vendor TPM chipset firmware and not caused due to Microsoft Windows.

The target system is missing defence in depth patches released by Microsoft to help work around the vulnerability by generating software-based keys whenever possible. The update helps to prevent generation of weak keys by the TPM hardware. It is recommended to implement additional remediation steps, even after applying the patches.to force regeneration of previously created weak TPM keys.

Successful exploitation allows attackers to determine the private key,

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.

130793 - Debian Linux 8.0 DSA-3886-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-1000364, CVE-2017-7487, CVE-2017-7645, CVE-2017-7895, CVE-2017-8064, CVE-2017-8890, CVE-2017-8924,

CVE-2017-8925, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242

Update Details

CVE is updated

163414 - Oracle Enterprise Linux ELSA-2017-2192 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6662, CVE-2016-6664, CVE-2017-3238, CVE-2017-3243, CVE-2017-3244, CVE-2017-3258, CVE-2017-3265, CVE-2017-3291, CVE-2017-3302, CVE-2017-3308, CVE-2017-3309, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3453, CVE-2017-3456, CVE-2017-3464, CVE-2017-3600, CVE-2017-3651

Update Details

CVE is updated

185731 - Ubuntu Linux 16.04 USN-3312-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7913, CVE-2016-7917, CVE-2016-8632, CVE-2016-9083, CVE-2016-9084, CVE-2016-9604, CVE-2017-2596, CVE-2017-2671, CVE-2017-6001, CVE-2017-7472, CVE-2017-7618, CVE-2017-7645, CVE-2017-7889, CVE-2017-7895

Update Details

CVE is updated

185735 - Ubuntu Linux 14.04 USN-3312-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-7913, CVE-2016-7917, CVE-2016-8632, CVE-2016-9083, CVE-2016-9084, CVE-2016-9604, CVE-2017-2596, CVE-2017-2671, CVE-2017-6001, CVE-2017-7472, CVE-2017-7618, CVE-2017-7645, CVE-2017-7889, CVE-2017-7895

Update Details

CVE is updated

185738 - Ubuntu Linux 17.04 USN-3314-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-9604, CVE-2017-2671, CVE-2017-7277, CVE-2017-7472, CVE-2017-7618, CVE-2017-7645, CVE-2017-7889, CVE-2017-7895, CVE-2017-7979, CVE-2017-8063, CVE-2017-8064, CVE-2017-8067

Update Details

CVE is updated

185752 - Ubuntu Linux 14.04 USN-3335-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9940, CVE-2017-1000363, CVE-2017-1000364, CVE-2017-7294, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242

Update Details

CVE is updated

185765 - Ubuntu Linux 14.04 USN-3343-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9940, CVE-2017-1000363, CVE-2017-7294, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242

Update Details

CVE is updated

185732 - Ubuntu Linux 16.10 USN-3313-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

CVE is updated

185736 - Ubuntu Linux 16.04 USN-3313-2 Update Is Not Installed

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Update Details

CVE is updated

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

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

Risk Level: High

CVE: CVE-2017-8695

Update Details

FASLScript is updated

22473 - (VMSA-2017-0015) VMware Workstation Player Multiple Vulnerabilities

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

Risk Level: High

CVE: CVE-2017-4924, CVE-2017-4925

Update Details

Risk is updated

22474 - (VMSA-2017-0015) VMware Workstation Player Multiple Vulnerabilities II

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-4924, CVE-2017-4925

Update Details

Risk is updated

22502 - (VMSA-2017-0015) VMware Workstation Player Multiple Vulnerabilities III

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

Risk Level: High

CVE: CVE-2017-4924, CVE-2017-4925

Update Details

Risk is updated

22503 - (VMSA-2017-0015) VMware Workstation Player Multiple Vulnerabilities IV

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-4924, CVE-2017-4925

Update Details

Risk is updated

141723 - Red Hat Enterprise Linux RHSA-2017-2787 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-6664, CVE-2016-8327, CVE-2017-3238, CVE-2017-3244, CVE-2017-3257, CVE-2017-3258, CVE-2017-3265, CVE-2017-3273, CVE-2017-3291, CVE-2017-3302, CVE-2017-3305, CVE-2017-3308, CVE-2017-3309, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3450, CVE-2017-3452, CVE-2017-3453, CVE-2017-3456, CVE-2017-3461, CVE-2017-3462, CVE-2017-3463, CVE-2017-3464, CVE-2017-3599, CVE-2017-3600, CVE-2017-3633, CVE-2017-3634, CVE-2017-3636, CVE-2017-3641, CVE-2017-3647, CVE-2017-3648, CVE-2017-3649, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653

Update Details

CVE is updated

145485 - SuSE SLES 12 SP3 SUSE-SU-2017:2202-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10978, CVE-2017-10983, CVE-2017-10984, CVE-2017-10985, CVE-2017-10986, CVE-2017-10987

Update Details

CVE is updated

145499 - SuSE SLES 12 SP2 SUSE-SU-2017:2243-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10978, CVE-2017-10983, CVE-2017-10984, CVE-2017-10985, CVE-2017-10987

Update Details

CVE is updated

145538 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1209-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-3302, CVE-2017-3305, CVE-2017-3308, CVE-2017-3309, CVE-2017-3329, CVE-2017-3450, CVE-2017-3452, CVE-2017-3453, CVE-2017-3456, CVE-2017-3461, CVE-2017-3462, CVE-2017-3463, CVE-2017-3464, CVE-2017-3599, CVE-2017-3600

Update Details

CVE is updated

145547 - SuSE Linux 42.3 openSUSE-SU-2017:2270-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-10978, CVE-2017-10983, CVE-2017-10984, CVE-2017-10985, CVE-2017-10986, CVE-2017-10987

Update Details

CVE is updated

145701 - SuSE Linux 42.1 openSUSE-SU-2017:0397-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10128, CVE-2016-10129, CVE-2016-10130

Update Details

CVE is updated

145746 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2337-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10397, CVE-2016-5766, CVE-2017-11142, CVE-2017-11144, CVE-2017-11145, CVE-2017-11147, CVE-2017-11628, CVE-2017-7890

Update Details

CVE is updated

145798 - SuSE Linux 42.1, 42.2 openSUSE-SU-2017:1196-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10195, CVE-2016-10196, CVE-2016-10197, CVE-2017-5398, CVE-2017-5399, CVE-2017-5400, CVE-2017-5401, CVE-2017-5402, CVE-2017-5403, CVE-2017-5404, CVE-2017-5405, CVE-2017-5406, CVE-2017-5407, CVE-2017-5408, CVE-2017-

5410, CVE-2017-5412, CVE-2017-5413, CVE-2017-5414, CVE-2017-5416, CVE-2017-5418, CVE-2017-5419, CVE-2017-5421, CVE-2017-5422, CVE-2017-5426, CVE-2017-5429, CVE-2017-5430, CVE-2017-5432, CVE-2017-5433, CVE-2017-5434, CVE-2017-5435, CVE-2017-5436, CVE-2017-5438, CVE-2017-5439, CVE-2017-5440, CVE-2017-5441, CVE-2017-5442, CVE-2017-5443, CVE-2017-5444, CVE-2017-5445, CVE-2017-5446, CVE-2017-5447, CVE-2017-5449, CVE-2017-5451, CVE-2017-5454, CVE-2017-5459, CVE-2017-5460, CVE-2017-5461, CVE-2017-5462, CVE-2017-5464, CVE-2017-5465, CVE-2017-5466, CVE-2017-5467, CVE-2017-5469

Update Details

CVE is updated

145817 - SuSE Linux 42.2 openSUSE-SU-2017:0484-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10128, CVE-2016-10129, CVE-2016-10130

Update Details

CVE is updated

145929 - SuSE SLES 11 SP4 SUSE-SU-2017:2522-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-10168, CVE-2016-10397, CVE-2016-5766, CVE-2017-11144, CVE-2017-11145, CVE-2017-11147, CVE-2017-11628, CVE-2017-12933, CVE-2017-7890

Update Details

CVE is updated

160305 - CentOS 6 CESA-2017-2795 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes

Risk Level: High

CVE: CVE-2017-1000253

Update Details

CVE is updated

181423 - FreeBSD proxychains-ng Current Path As The First Directory For The Library Search Path (9471ec47-05a2-11e5-8fda-002590263bf5)

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

Risk Level: High

CVE: CVE-2015-3887

Update Details

Risk is updated

182452 - FreeBSD perl Multiple Vulnerabilities (d9e82328-a129-11e7-987e-4f174049b30a)

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

Risk Level: High

CVE: CVE-2017-12814, CVE-2017-12837, CVE-2017-12883

Update Details

Risk is updated

130875 - Debian Linux 8.0, 9.0 DSA-3970-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14482

Update Details

Risk is updated

130883 - Debian Linux 8.0, 9.0 DSA-3977-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14500

Update Details

Risk is updated

130886 - Debian Linux 9.0 DSA-3975-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14482

Update Details

Risk is updated

130889 - Debian Linux 8.0, 9.0 DSA-3982-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-12837, CVE-2017-12883

Update Details

Risk is updated

141667 - Red Hat Enterprise Linux RHSA-2017-2192 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-6664, CVE-2017-3238, CVE-2017-3243, CVE-2017-3244, CVE-2017-3258, CVE-2017-3265, CVE-2017-3291, CVE-2017-3302, CVE-2017-3308, CVE-2017-3309, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3453, CVE-2017-3456, CVE-2017-3464, CVE-2017-3600

Update Details

CVE is updated

141718 - Red Hat Enterprise Linux RHSA-2017-2771 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14482

Update Details

Risk is updated

142049 - SuSE Linux 13.1 openSUSE-SU-2014:0333-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-2029

Update Details

Risk is updated

142069 - SuSE Linux 13.1 openSUSE-SU-2014:0363-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2014-2029

Update Details

Risk is updated

145678 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2366-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-10397, CVE-2016-5766, CVE-2017-11143, CVE-2017-11144, CVE-2017-11145, CVE-2017-11147, CVE-2017-11628, CVE-2017-7890

Update Details

CVE is updated

145933 - SuSE SLES 11 SP4 SUSE-SU-2017:2532-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14482

Update Details

Risk is updated

145939 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2535-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14482

Update Details

Risk is updated

145942 - SuSE SLES 12 SP2, 12 SP3, SLED 12 SP2, 12 SP3 SUSE-SU-2017:2529-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14482

Update Details

Risk is updated

163456 - Oracle Enterprise Linux ELSA-2017-2771 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-14482

Update Details

Risk is updated

175220 - Scientific Linux Security ERRATA Moderate: mariadb on SL7.x x86_64 (1708-14039)

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

Risk Level: Medium

CVE: CVE-2016-6664, CVE-2017-3238, CVE-2017-3243, CVE-2017-3244, CVE-2017-3258, CVE-2017-3265, CVE-2017-3291, CVE-2017-3302, CVE-2017-3308, CVE-2017-3309, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3453, CVE-2017-3456, CVE-2017-3464, CVE-2017-3600

Update Details

CVE is updated

175261 - Scientific Linux Security ERRATA Important: emacs on SL7.x x86_64 (1709-1762)

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

Risk Level: Medium

CVE: CVE-2017-14482

Update Details

Risk is updated

181486 - FreeBSD devel/ipython CSRF Possible Remote Execution Vulnerability (81326883-2905-11e5-a4a5-002590263bf5)

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

Risk Level: Medium

CVE: CVE-2015-5607

Update Details

Risk is updated

182445 - FreeBSD rubygem-geminabox XSS & CSRF Vulnerabilities (2bffdf2f-9d45-11e7-a25c-471bafc3262f)

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-14506, CVE-2017-14683

Update Details
Risk is updated

189587 - Fedora Linux 21 FEDORA-2015-11767 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-5607

Update Details
Risk is updated

189593 - Fedora Linux 22 FEDORA-2015-11677 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-5607

Update Details
Risk is updated

192635 - Fedora Linux 25 FEDORA-2017-3a568adb31 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-14482

Update Details
Risk is updated

85906 - CentOS 7 CESA-2015-0895 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Cent OS Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-1854

Update Details
Risk is updated

91787 - Oracle Enterprise Linux ELSA-2015-0895 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Oracle Enterprise Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-1854

Update Details

Risk is updated

130891 - Debian Linux 8.0, 9.0 DSA-3980-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-9798

Update Details
Risk is updated

145936 - SuSE SLES 12 SP2, 12 SP3 SUSE-SU-2017:2542-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-9798

Update Details
Risk is updated

145937 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2549-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-9798

Update Details
Risk is updated

170516 - Amazon Linux AMI ALAS-2015-538 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-1854

Update Details
Risk is updated

170872 - Amazon Linux AMI ALAS-2017-896 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Amazon Linux Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-9798

Update Details
Risk is updated

182442 - FreeBSD Apache HTTP OPTIONS Method Can Leak Server Memory (76b085e2-9d33-11e7-9260-000c292ee6b8)

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

CVE: CVE-2017-9798

Update Details

Risk is updated

182451 - FreeBSD weechat Crash In Logger Plugin (b63421b6-a1e0-11e7-ac58-b499baebfeaf)

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

Risk Level: Medium

CVE: CVE-2017-14727

Update Details

Risk is updated

185884 - Ubuntu Linux 14.04, 16.04, 17.04 USN-3425-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9798

Update Details

Risk is updated

189295 - Fedora Linux 22 FEDORA-2015-7206 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1854

Update Details

Risk is updated

192668 - Fedora Linux 26 FEDORA-2017-a52f252521 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-9798

Update Details

Risk is updated

91932 - Oracle Enterprise Linux ELSA-2015-2369 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3248

Update Details

Risk is updated

130777 - Debian Linux 8.0 DSA-3865-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-7650

Update Details

Risk is updated

141005 - Red Hat Enterprise Linux RHSA-2015-2369 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3248

Update Details

Risk is updated

143576 - SuSE Linux 13.1, 13.2 openSUSE-SU-2015:0472-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-1027

Update Details

Risk is updated

145951 - SuSE Linux 42.2, 42.3 openSUSE-SU-2017:2573-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2017-0380

Update Details

Risk is updated

174864 - Scientific Linux Security ERRATA Low: openhpi on SL7.x x86_64 (1512-8750)

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

Risk Level: Medium

CVE: CVE-2015-3248

Update Details

Risk is updated

181465 - FreeBSD wesnoth Disclosure Of .pbl Files With Lowercase, Uppercase, And Mixed-case Extension (2a8b7d21-1ecc-11e5-a4a5-002590263b

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

Risk Level: Medium

CVE: CVE-2015-5069, CVE-2015-5070

Update Details

Risk is updated

189248 - Fedora Linux 22 FEDORA-2015-7156 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3420

Update Details

Risk is updated

189336 - Fedora Linux 20 FEDORA-2015-7159 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3420

Update Details

Risk is updated

189338 - Fedora Linux 21 FEDORA-2015-7089 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-3420

Update Details

Risk is updated

189506 - Fedora Linux 21 FEDORA-2015-10973 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5069, CVE-2015-5070

Update Details

Risk is updated

189514 - Fedora Linux 22 FEDORA-2015-10964 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-5069, CVE-2015-5070

Update Details

Risk is updated

189808 - Fedora Linux 22 FEDORA-2015-10944 Update Is Not Installed

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

Risk Level: Medium
CVE: CVE-2015-3248

Update Details
Risk is updated

192181 - Fedora Linux 26 FEDORA-2017-59f85fef2c Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-7650

Update Details
Risk is updated

192185 - Fedora Linux 24 FEDORA-2017-486a536b62 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-7650

Update Details
Risk is updated

192222 - Fedora Linux 25 FEDORA-2017-c2113aacd2 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-7650

Update Details
Risk is updated

130877 - Debian Linux 9.0 DSA-3965-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes
Risk Level: Low
CVE: CVE-2017-1000249

Update Details
Risk is updated

185869 - Ubuntu Linux 17.04 USN-3412-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Low
CVE: CVE-2017-1000249

Update Details
Risk is updated

192630 - Fedora Linux 26 FEDORA-2017-bb4c07b01a Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2017-1000249

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.