2017-APR-11
FSL version 7.5.910

# 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

### 21635 - (APSB17-10) Vulnerabilities In Adobe Flash Player

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

Risk Level: High

CVE: CVE-2017-3058, CVE-2017-3059, CVE-2017-3060, CVE-2017-3061, CVE-2017-3062, CVE-2017-3063, CVE-2017-3064

Description

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

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws occur due to multiple logic and memory issues. Successful exploitation could allow an attacker to execute remote code or retrieve sensitive data from the target system.

The update provided by Adobe bulletin APSB17-10 resolves the issues. The target system is missing this update.

### 21636 - (APSB17-10) Vulnerabilities In Adobe Flash Player

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2017-3058, CVE-2017-3059, CVE-2017-3060, CVE-2017-3061, CVE-2017-3062, CVE-2017-3063, CVE-2017-3064

Description

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

Observation

Adobe Flash Player is a software application used for viewing rich Internet applications, streaming audio, video and multimedia files.

Multiple vulnerabilities are present in some versions of Adobe Flash Player. The flaws occur due to multiple logic and memory issues. Successful exploitation could allow an attacker to execute remote code or retrieve sensitive data from the target system.

The update provided by Adobe bulletin APSB17-10 resolves the issues. The target system is missing this update.

### 21593 - Microsoft Edge Security Bypass (4015217)

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

Risk Level: High

CVE: CVE-2017-0203

Description

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

Observation

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

The flaw exists when the Edge Content Security Policy (CSP) fails to properly validate certain specially crafted documents. Successful exploitation could allow a remote attacker to bypass intended access restrictions.

## 21594 - Microsoft Edge Memory Corruption Remote Code Execution (4015583)

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

Risk Level: High

CVE: CVE-2017-0205

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 exists when Microsoft Edge improperly accesses objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

## 21603 - Microsoft .NET Remote Code Execution (4015549)

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

Risk Level: High

CVE: CVE-2017-0160

Description

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

Observation

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

The flaw exists when Microsoft .NET Framework fails to properly validate input before loading libraries. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

## 21604 - Microsoft Internet Explorer Memory Corruption Remote Code Execution (4015550)

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

Risk Level: High

CVE: CVE-2017-0202

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 exists when Internet Explorer improperly accesses objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

## 21617 - Microsoft Hyper-V Remote Code Execution I (4015547)

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

Risk Level: High

CVE: CVE-2017-0162

Description

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

Observation

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

The flaw exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system. Successful exploitation by a local attacker could result in the execution of arbitrary code.

## 21618 - Microsoft Hyper-V Remote Code Execution II (4015547)

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

Risk Level: High

CVE: CVE-2017-0163

Description

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

Observation

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

The flaw exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system. Successful exploitation by a local attacker could result in the execution of arbitrary code.

## 21620 - Microsoft Hyper-V Remote Code Execution III (4015547)

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

Risk Level: High

CVE: CVE-2017-0181

Description

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

Observation

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

The flaw exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system. Successful exploitation by a local attacker could result in the execution of arbitrary code.

## 21627 - Microsoft Internet Explorer Privilege Escalation (4015550)

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

Description

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

Observation

An elevation of privilege vulnerability exists when Microsoft Internet Explorer does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain.In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability. An attacker who successfully exploited this vulnerability could elevate privileges in affected versions of Internet Explorer.

## 21634 - (APSB17-11) Vulnerabilities In Adobe Reader And Acrobat

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

Risk Level: High

CVE: CVE-2017-3011, CVE-2017-3012, CVE-2017-3013, CVE-2017-3014, CVE-2017-3015, CVE-2017-3017, CVE-2017-3018, CVE-2017-3019, CVE-2017-3020, CVE-2017-3021, CVE-2017-3022, CVE-2017-3023, CVE-2017-3024, CVE-2017-3025, CVE-2017-3026, CVE-2017-3027, CVE-2017-3028, CVE-2017-3029, CVE-2017-3030, CVE-2017-3031, CVE-2017-3032, CVE-2017-3033, CVE-2017-3034, CVE-2017-3035, CVE-2017-3036, CVE-2017-3037, CVE-2017-3038, CVE-2017-3039, CVE-2017-3040, CVE-2017-3041, CVE-2017-3042, CVE-2017-3043, CVE-2017-3044, CVE-2017-3045, CVE-2017-3046, CVE-2017-3047, CVE-2017-3048, CVE-2017-3049, CVE-2017-3050, CVE-2017-3051, CVE-2017-3052, CVE-2017-3053, CVE-2017-3054, CVE-2017-3055, CVE-2017-3056, CVE-2017-3057, CVE-2017-3065

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 information.

The update provided by Adobe bulletin APSB17-11 resolves these issues. The target system appears to be missing this update.

## 21584 - Microsoft Outlook Parsing Remote Code Execution I

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

Risk Level: High

CVE: CVE-2017-0106

Description

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

Observation

A vulnerability in some versions of Microsoft Outlook could lead to remote code execution.  The flaw lies in the Parsing 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.

## 21587 - Microsoft Office DLL Loading Remote Code Execution

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

Risk Level: High

CVE: CVE-2017-0197

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 DLL Loading 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.

## 21588 - Microsoft Outlook Parsing Remote Code Execution II

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

Risk Level: High

CVE: CVE-2017-0199

Description

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

Observation

A vulnerability in some versions of Microsoft Outlook could lead to remote code execution. The flaw lies in the Parsing 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.

## 21592 - Microsoft Windows Memory Handling Denial of Service

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

Risk Level: High

CVE: CVE-2017-0191

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 a memory handling error. 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.

## 21595 - Microsoft Edge Scripting Engine Remote Code Execution III

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

Risk Level: High

CVE: CVE-2017-0093

Description

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

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution. The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

## 21596 - Microsoft Edge Scripting Engine Remote Code Execution V

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

Risk Level: High

CVE: CVE-2017-0200

Description

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

Observation

A vulnerability in some versions of Microsoft Edge could lead to remote code execution. The flaw lies in the Scripting Engine component. Successful exploitation by a remote attacker could result in the execution of arbitrary code. The exploit requires the user to open a vulnerable website, email or document.

## 21605 - Microsoft Internet Explorer Scripting Engine Remote Code Execution

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

Risk Level: High

CVE: CVE-2017-0201

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.

## 21606 - Microsoft Internet Explorer Scripting Engine Remote Code Execution II

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

Risk Level: High

CVE: CVE-2017-0158

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.

## 21619 - Microsoft Windows Hyper-V Remote Code Execution

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

Risk Level: High

CVE: CVE-2017-0180

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

## 21583 - Microsoft Office Spoofing

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2017-0207

Description

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

Observation

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

The flaw occurs when Microsoft Outlook improperly validates HTML tag input.

## 21585 - Microsoft Office Memory Corruption Information Disclosure

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

Risk Level: Medium

CVE: CVE-2017-0194

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 exists when Microsoft Office improperly discloses the contents of its memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

## 21586 - Microsoft Office Cross Site Scripting Privilege Escalation

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

Risk Level: Medium

CVE: CVE-2017-0195

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 a cross site scripting error.Successful exploitation could allow a local user to gain elevated privileges. The exploit requires the user to open a vulnerable website, email or document.

### 21589 - Microsoft Office File Parsing Security Bypass

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

Risk Level: Medium

CVE: CVE-2017-0204

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

### 21590 - Microsoft Active Directory Denial of Service (4015217)

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

Risk Level: Medium

CVE: CVE-2017-0164

Description

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

Observation

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

The flaw occurs in Active Directory when an authenticated attacker creates multiple machine accounts. Successful exploitation by a local attacker could result in a denial of service condition.

### 21591 - Microsoft Windows Kernel Information Disclosure V

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

Risk Level: Medium

CVE: CVE-2017-0167

Description

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

Observation

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

## 21597 - Microsoft Windows Kernel Information Disclosure III

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

Risk Level: Medium

CVE: CVE-2017-0058

Description

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

Observation

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

## 21598 - Microsoft Windows Kernel Privilege Escalation II

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

Risk Level: Medium

CVE: CVE-2017-0189

Description

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

Observation

A vulnerability in some versions of Microsoft Windows could lead to privilege escalation. The flaw lies in the Kernel component.Successful exploitation could allow a local user to gain elevated privileges.The exploit requires the attacker to have valid credentials to the vulnerable system.

## 21599 - Microsoft Windows Kernel Information Disclosure IV

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

Risk Level: Medium

CVE: CVE-2017-0188

Description

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

Observation

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

## 21600 - Microsoft ATMFD.dll Information Disclosure (4015380)

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

Risk Level: Medium

CVE: CVE-2017-0192

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 occurs when ATMFD.dll fails to properly handle objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

### 21601 - Microsoft Windows Graphics Privilege Escalation

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

Risk Level: Medium

CVE: CVE-2017-0155

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 user to open a vulnerable website, email or document.

### 21602 - Microsoft Windows Handle Sanitization Privilege Escalation

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

Risk Level: Medium

CVE: CVE-2017-0165

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

### 21607 - Microsoft Edge Scripting Engine Information Disclosure

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

Risk Level: Medium

CVE: CVE-2017-0208

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 occurs when the Chakra scripting engine does not properly handle objects in memory. Successful exploitation by a remote

attacker could result in the disclosure of sensitive information.

### 21608 - Microsoft Hyper-V Denial of Service I (4015547)

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

Risk Level: Medium

CVE: CVE-2017-0178

Description

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

Observation

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

The flaw exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. Successful exploitation by a remote attacker could result in a denial of service condition.

### 21609 - Microsoft Hyper-V Denial of Service II (4015547)

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

Risk Level: Medium

CVE: CVE-2017-0179

Description

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

Observation

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

The flaw exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. Successful exploitation by a remote attacker could result in a denial of service condition.

### 21610 - Microsoft Hyper-V Denial of Service III (4015547)

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

Risk Level: Medium

CVE: CVE-2017-0182

Description

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

Observation

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

The flaw exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. Successful exploitation by a remote attacker could result in a denial of service condition.

### 21611 - Microsoft Hyper-V Denial of Service IV (4015547)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2017-0183

Description

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

Observation

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

The flaw exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. Successful exploitation by a remote attacker could result in a denial of service condition.

### 21612 - Microsoft Hyper-V Denial of Service V (4015547)

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

Risk Level: Medium

CVE: CVE-2017-0184

Description

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

Observation

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

The flaw exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. Successful exploitation by a remote attacker could result in a denial of service condition.

### 21613 - Microsoft Hyper-V Denial of Service VI (4015547)

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

Risk Level: Medium

CVE: CVE-2017-0185

Description

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

Observation

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

The flaw exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. Successful exploitation by a remote attacker could result in a denial of service condition.

### 21614 - Microsoft Hyper-V Denial of Service VII (4015547)

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

Risk Level: Medium

CVE: CVE-2017-0186

Description

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

Observation

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

The flaw exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system. Successful exploitation by a remote attacker could result in a denial of service condition.

### 21615 - Microsoft Hyper-V Information Disclosure I (4015547)

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

Risk Level: Medium

CVE: CVE-2017-0168

Description

A vulnerability in some versions of Microsoft Hyper-V could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Hyper-V could lead to information disclosure.

The flaw exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

### 21616 - Microsoft Hyper-V Information Disclosure II (4015547)

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

Risk Level: Medium

CVE: CVE-2017-0169

Description

A vulnerability in some versions of Microsoft Hyper-V could lead to information disclosure.

Observation

A vulnerability in some versions of Microsoft Hyper-V could lead to information disclosure.

The flaw exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

### 21621 - Microsoft Windows libjpeg Information Disclosure (4015383)

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

Risk Level: Medium

CVE: CVE-2013-6629

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 exists within the open-source libjpeg image-processing library where it fails to properly handle objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

### 21622 - Microsoft LDAP Privilege Escalation (4015547)

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

Risk Level: Medium

CVE: CVE-2017-0166

Description

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

Observation

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

The flaw exists when LDAP request buffer lengths are improperly calculated. Successful exploitation could allow a local user to gain elevated privileges.

### 21623 - Microsoft ADFS Security Bypass (4015217)

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

Risk Level: Medium

CVE: CVE-2017-0159

Description

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

Observation

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

The flaw exists when ADFS incorrectly treats requests coming from Extranet clients as Intranet requests. Successful exploitation could allow a remote attacker to bypass intended access restrictions.

### 21626 - Microsoft Windows OLE Privilege Escalation

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

Risk Level: Medium

CVE: CVE-2017-0211

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 occurs in Microsoft Windows OLE when it fails an integrity-level check. Successful exploitation could allow a local user to gain elevated privileges.

### 21628 - Microsoft Windows Graphics Privilege Escalation II

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

Risk Level: Medium

CVE: CVE-2017-0156

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 occurs when the Microsoft Graphics Component fails to properly handle objects in memory. Successful exploitation could allow a local user to gain elevated privileges.

## 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.

### 93524 - Mandriva Linux MBS2 MDVSA-2015-122 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9114

Update Details

Risk is updated

### 130169 - Debian Linux 7.0 DSA-3248-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-5008

Update Details

Risk is updated

### 130729 - Debian Linux 8.0 DSA-3823-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6964

Update Details

Risk is updated

### 178256 - Gentoo Linux GLSA-201612-14 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9114

Update Details

Risk is updated

### 178413 - Gentoo Linux GLSA-201703-03 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6542

Update Details

Risk is updated

### 182308 - FreeBSD irssi Use-after-free Potential Code Execution (06f931c0-0be0-11e7-b4bf-5404a68ad561)

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

Risk Level: High

CVE: CVE-2017-7191

Update Details

Risk is updated

### 182310 - FreeBSD PuTTY Integer Overflow Permits Memory Overwrite By Forwarded Ssh-agent Connections (9b973e97-0a99-11e7-ace7-080027ef73ec

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

Risk Level: High

CVE: CVE-2017-6542

Update Details

Risk is updated

### 185639 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3246-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2017-6964

Update Details

Risk is updated

### 188609 - Fedora Linux 20 FEDORA-2014-16016 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2014-9114

Update Details

Risk is updated

### 188663 - Fedora Linux 21 FEDORA-2014-15908 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2014-9114

Update Details
Risk is updated

### 178278 - Gentoo Linux GLSA-201612-31 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-2015-8026

Update Details
Risk is updated

### 178381 - Gentoo Linux GLSA-201701-69 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Gentoo Linux Patches and HotFixes
Risk Level: Medium
CVE: CVE-2017-5330

Update Details
Risk is updated

### 185646 - Ubuntu Linux 16.04, 16.10 USN-3255-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-7358

Update Details
Risk is updated

### 191637 - Fedora Linux 25 FEDORA-2017-77ab791c90 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-5330

Update Details
Risk is updated

### 191867 - Fedora Linux 25 FEDORA-2017-5ebac1c112 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-6451, CVE-2017-6458, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464

Update Details
Risk is updated

**181460 - FreeBSD chicken Potential Buffer Overrun In String-translate* (0da404ad-1891-11e5-a1cf-002590263bf5)**

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-4556

Update Details
Risk is updated

**182204 - FreeBSD py-cryptography Vulnerable HKDF Key Generation (e5dcb942-ba6f-11e6-b1cf-14dae9d210b8)**

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-9243

Update Details
Risk is updated

**182319 - FreeBSD django Multible Vulnerabilities (dc880d6c-195d-11e7-8c63-0800277dcc69)**

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-7233, CVE-2017-7234

Update Details
Risk is updated

**185490 - Ubuntu Linux 16.04, 16.10 USN-3138-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-9243

Update Details
Risk is updated

**185658 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3254-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-7233, CVE-2017-7234

Update Details
Risk is updated

**189479 - Fedora Linux 21 FEDORA-2015-10165 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2015-4556

Update Details

Risk is updated

### 189481 - Fedora Linux 22 FEDORA-2015-10333 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-4556

Update Details

Risk is updated

### 190709 - Fedora Linux 24 FEDORA-2016-b86ae2068d Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4912

Update Details

Risk is updated

### 190794 - Fedora Linux 23 FEDORA-2016-d9dbd6d339 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4912

Update Details

Risk is updated

### 190946 - Fedora Linux 22 FEDORA-2016-33ad3f97d4 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-4912

Update Details

Risk is updated

### 191364 - Fedora Linux 24 FEDORA-2016-d3a2b640ce Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-9243

Update Details

Risk is updated

### 191374 - Fedora Linux 23 FEDORA-2016-e77c8c1f3b Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-9243

Update Details
Risk is updated

### 191398 - Fedora Linux 25 FEDORA-2016-2d90e27e50 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2016-9243

Update Details
Risk is updated

### 185640 - Ubuntu Linux 12.04, 14.04, 16.04, 16.10 USN-3247-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-6507

Update Details
Risk is updated

### 191876 - Fedora Linux 24 FEDORA-2017-66593c367e Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: Medium
CVE: CVE-2017-6503, CVE-2017-6504

Update Details
Risk is updated

### 185613 - Ubuntu Linux 14.04, 16.04, 16.10 USN-3224-1 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Ubuntu Patches and Hotfixes
Risk Level: Low
CVE: CVE-2017-5985

Update Details
Risk is updated

### 70046 - macosx.fasl3.inc

Category: General Vulnerability Assessment -> NonIntrusive -> Invalid Category
Risk Level: Informational
CVE: CVE-MAP-NOMATCH

Update Details
FASLScript is updated

## HOW TO UPDATE

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

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

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

## MCAFEE TECHNICAL SUPPORT

ServicePortal: https://mysupport.mcafee.com

Multi-National Phone Support available here:

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

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