

## MCAFFEE 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

#### 20655 - (APSB16-33) Vulnerabilities In Adobe Reader And Acrobat

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

Risk Level: High

CVE: CVE-2016-1089, CVE-2016-1091, CVE-2016-6939, CVE-2016-6940, CVE-2016-6941, CVE-2016-6942, CVE-2016-6943, CVE-2016-6944, CVE-2016-6945, CVE-2016-6946, CVE-2016-6947, CVE-2016-6948, CVE-2016-6949, CVE-2016-6950, CVE-2016-6951, CVE-2016-6952, CVE-2016-6953, CVE-2016-6954, CVE-2016-6955, CVE-2016-6956, CVE-2016-6957, CVE-2016-6958, CVE-2016-6959, CVE-2016-6960, CVE-2016-6961, CVE-2016-6962, CVE-2016-6963, CVE-2016-6964, CVE-2016-6965, CVE-2016-6966, CVE-2016-6967, CVE-2016-6968, CVE-2016-6969, CVE-2016-6970, CVE-2016-6971, CVE-2016-6972, CVE-2016-6973, CVE-2016-6974, CVE-2016-6975, CVE-2016-6976, CVE-2016-6977, CVE-2016-6978, CVE-2016-6979, CVE-2016-6988, CVE-2016-6993, CVE-2016-6994, CVE-2016-6995, CVE-2016-6996, CVE-2016-6997, CVE-2016-6998, CVE-2016-6999, CVE-2016-7000, CVE-2016-7001, CVE-2016-7002, CVE-2016-7003, CVE-2016-7004, CVE-2016-7005, CVE-2016-7006, CVE-2016-7007, CVE-2016-7008, CVE-2016-7009, CVE-2016-7010, CVE-2016-7011, CVE-2016-7012, CVE-2016-7013, CVE-2016-7014, CVE-2016-7015, CVE-2016-7016, CVE-2016-7017, CVE-2016-7018, CVE-2016-7019

#### 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 bypass security restrictions.

The update provided by Adobe bulletin APSB16-33 resolves these issues. The target system appears to be missing this update.

#### 20624 - (MS16-119) Cumulative Security Update for Microsoft Edge (3192890)

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

Risk Level: High

CVE: CVE-2016-3267, CVE-2016-3331, CVE-2016-3382, CVE-2016-3386, CVE-2016-3387, CVE-2016-3388, CVE-2016-3389, CVE-2016-3390, CVE-2016-3391, CVE-2016-3392, CVE-2016-7189, CVE-2016-7190, CVE-2016-7194

#### Description

Multiple vulnerabilities are present in some versions of Microsoft Edge.

#### Observation

Microsoft Edge is a web browser introduced in Microsoft Windows 10.

Multiple vulnerabilities are present in some versions of Microsoft Edge. The flaws lie in how this product processes objects in memory. Successful exploitation could allow an attacker to execute arbitrary code or obtain sensitive information.

Microsoft has provided MS16-119 to address these issues. The host appears to be missing this patch.

#### **20628 - (MS16-119) Microsoft Edge Browser Information Disclosure II (3192890)**

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

Risk Level: High

CVE: CVE-2016-7189

##### 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 Microsoft Edge does not properly handle objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

#### **20631 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution IV (3192890)**

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

Risk Level: High

CVE: CVE-2016-7190

##### 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 occurs in the way that the Chakra JavaScript engine renders when handling objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

#### **20632 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution III (3192890)**

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

Risk Level: High

CVE: CVE-2016-3390

##### 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 occurs in the way that the Chakra JavaScript engine renders when handling objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

#### **20633 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution II (3192890)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3389

#### 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 occurs in the way that the Chakra JavaScript engine renders when handling objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

### **20634 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution I (3192890)**

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

Risk Level: High

CVE: CVE-2016-3386

#### 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 occurs in the way that the Chakra JavaScript engine renders when handling objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

### **20635 - (MS16-119) Microsoft Edge Browser Memory Corruption Remote Code Execution II (3192890)**

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

Risk Level: High

CVE: CVE-2016-3382

#### 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 occurs in the way that Microsoft Edge handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

### **20636 - (MS16-119) Microsoft Edge Browser Memory Corruption Remote Code Execution I (3192890)**

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

Risk Level: High

CVE: CVE-2016-3331

#### 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 occurs in the way that Microsoft Edge handles objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

### **20653 - (APSB16-32) Vulnerabilities In Adobe Flash Player**

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

Risk Level: High

CVE: CVE-2016-4273, CVE-2016-4286, CVE-2016-6981, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6987, CVE-2016-6989, CVE-2016-6990, CVE-2016-6992

#### 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 bypass security access restrictions.

The update provided by Adobe bulletin APSB16-32 resolves the issues. The target system is missing this update.

### **20654 - (APSB16-32) Vulnerabilities In Adobe Flash Player**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-4273, CVE-2016-4286, CVE-2016-6981, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6987, CVE-2016-6989, CVE-2016-6990, CVE-2016-6992

#### 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 bypass security access restrictions.

The update provided by Adobe bulletin APSB16-32 resolves the issues. The target system is missing this update.

### **20663 - (MS16-119) Microsoft Edge Browser Scripting Engine Memory Corruption Remote Code Execution V (3192890)**

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

Risk Level: High

CVE: CVE-2016-7194

#### 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 occurs in the way that the Chakra JavaScript engine renders when handling objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

### **20666 - (MS16-118) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3192887)**

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

Risk Level: High

CVE: CVE-2016-3331

#### 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 occurs in the way that Internet Explorer accesses objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

### **20667 - (MS16-118) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3192887)**

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

Risk Level: High

CVE: CVE-2016-3382

#### 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 occurs in the way that Internet Explorer accesses objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

### **20668 - (MS16-118) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3192887)**

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

Risk Level: High

CVE: CVE-2016-3383

#### 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 occurs in the way that Internet Explorer accesses objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

#### **20669 - (MS16-118) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3192887)**

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

Risk Level: High

CVE: CVE-2016-3384

##### 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 occurs in the way that Internet Explorer accesses objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

#### **20670 - (MS16-118) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3192887)**

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

Risk Level: High

CVE: CVE-2016-3385

##### 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 occurs in the way that Internet Explorer accesses objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

#### **20673 - (MS16-118) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution (3192887)**

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

Risk Level: High

CVE: CVE-2016-3390

##### 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 occurs in the way that the Scripting Engine renders when handling objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

#### **20675 - (MS16-118) Cumulative Security Update for Internet Explorer (3192887)**

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

Risk Level: High

CVE: CVE-2016-3267, CVE-2016-3298, CVE-2016-3331, CVE-2016-3382, CVE-2016-3383, CVE-2016-3384, CVE-2016-3385, CVE-2016-3387, CVE-2016-3388, CVE-2016-3390, CVE-2016-3391

#### Description

Multiple vulnerabilities are present in some versions of Microsoft Internet Explorer.

#### Observation

Microsoft Internet Explorer is a popular web browser.

Multiple vulnerabilities are present in some versions of Microsoft Internet Explorer. The flaws lie in several components. Successful exploitation could allow an attacker to remotely execute arbitrary code, retrieve sensitive data or escalate privileges.

Microsoft has provided MS16-118 to address this issues. The host appears to be missing this patch.

### **20678 - (MS16-120) Security Update for Microsoft Graphics Component (3192884)**

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

Risk Level: High

CVE: CVE-2016-3209, CVE-2016-3262, CVE-2016-3263, CVE-2016-3270, CVE-2016-3393, CVE-2016-3396, CVE-2016-7182

#### Description

Multiple vulnerabilities are present in some versions of Microsoft Windows.

#### Observation

Microsoft Windows is an industry-standard operating system.

Multiple vulnerabilities are present in some versions of Microsoft Windows. The flaws lie in the Microsoft Graphics component. Successful exploitation could allow a remote attacker to obtain sensitive information, obtain elevated privileges or execute remote code.

Microsoft has provided MS16-120 to address these issues. The host appears to be missing this patch.

### **20679 - (MS16-120) Security Update for Microsoft Graphics Component (3192884)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-3209, CVE-2016-3262, CVE-2016-3263, CVE-2016-3270, CVE-2016-3393, CVE-2016-3396, CVE-2016-7182

#### Description

Multiple vulnerabilities are present in some versions of Microsoft Windows.

#### Observation

Microsoft Windows is an industry-standard operating system.

Multiple vulnerabilities are present in some versions of Microsoft Windows. The flaws lie in the Microsoft Graphics component. Successful exploitation could allow a remote attacker to obtain sensitive information, obtain elevated privileges or execute remote code.

Microsoft has provided MS16-120 to address these issues. The host appears to be missing this patch.

---

## 20685 - (MS16-120) Microsoft Windows Graphics GDI+ Remote Code Execution (3192884)

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

Risk Level: High

CVE: CVE-2016-3396

### Description

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

### Observation

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

The flaw occurs when the Windows font library improperly handles specially crafted embedded fonts. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

## 20686 - (MS16-120) Microsoft Windows Graphics Component Remote Code Execution (3192884)

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

Risk Level: High

CVE: CVE-2016-3393

### Description

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

### Observation

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

The flaw occurs due to the way the Windows GDI handles objects in the memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

## 20687 - (MS16-122) Security Update for Microsoft Video Control (3195360)

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

Risk Level: High

CVE: CVE-2016-0142

### Description

A vulnerability is present in some versions of Microsoft Windows.

### Observation

Microsoft Windows is an industry-standard operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw occurs when Microsoft Video Control fails to properly handle objects in memory. Successful exploitation could allow a remote attacker to execute of arbitrary code.

Microsoft has provided MS16-122 to address these issues. The host appears to be missing this patch.

## 20688 - (MS16-122) Microsoft Windows Video Control Remote Code Execution (3195360)



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

Risk Level: High

CVE: CVE-2016-0142

#### 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 occurs when exists when Microsoft Video Control fails to properly handle objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

### **20637 - (MS16-121) Security Update for Microsoft Office (3194063)**

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

Risk Level: High

CVE: CVE-2016-7193

#### Description

A vulnerability is present in some versions of Microsoft Office.

#### Observation

Microsoft Office is a popular office suite.

A vulnerability is present in some versions of Microsoft Office. The flaw lies in Office RTF files management. Successful exploitation could allow an attacker to execute arbitrary code affecting confidentiality, integrity or availability of the system.

Microsoft has provided MS16-121 to address this issue. The host appears to be missing this patch.

### **20638 - (MS16-121) Security Update for Microsoft Office (3194063)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-7193

#### Description

A vulnerability is present in some versions of Microsoft Office.

#### Observation

Microsoft Office is a popular office suite.

A vulnerability is present in some versions of Microsoft Office. The flaw lies in Office RTF files management. Successful exploitation could allow an attacker to execute arbitrary code affecting confidentiality, integrity or availability of the system.

Microsoft has provided MS16-121 to address this issue. The host appears to be missing this patch.

### **20640 - (MS16-123) Security Update for Windows Kernel-Mode Drivers (3192892)**

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3266, CVE-2016-3341, CVE-2016-3376, CVE-2016-7185, CVE-2016-7211

#### Description

Multiple vulnerabilities are present in some versions of Microsoft Windows.

#### Observation

Microsoft Windows is a popular operating system.

Multiple vulnerabilities are present in some versions of Microsoft Windows. The flaws occur when the Windows kernel-mode driver fails to properly handle objects in memory. Successful exploitation could allow a local user to gain elevated privileges.

Microsoft has provided MS16-123 to address these issues. The host appears to be missing this patch.

### **20647 - (MS16-124) Security Update for Windows Registry (3193227)**

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

Risk Level: High

CVE: CVE-2016-0070, CVE-2016-0073, CVE-2016-0075, CVE-2016-0079

#### Description

Multiple vulnerabilities are present in some versions of Microsoft Windows.

#### Observation

Microsoft Windows is a popular operating system.

Multiple vulnerabilities are present in some versions of Microsoft Windows. The flaws lie in the Windows Registry. Successful exploitation could allow an attacker to bypass security measures or retrieve sensitive data.

Microsoft has provided MS16-124 to address these issues. The host appears to be missing this patch.

### **20625 - (MS16-119) Microsoft Edge Browser Security Bypass (3192890)**

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

Risk Level: Medium

CVE: CVE-2016-3392

#### 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 occurs when Microsoft Edge fails to properly secure private namespace. Successful exploitation could allow a remote attacker to bypass intended access restrictions.

### **20626 - (MS16-119) Microsoft Edge Browser Privilege Escalation II (3192890)**

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

Risk Level: Medium  
CVE: CVE-2016-3387

#### Description

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

#### Observation

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

The flaw occurs when Microsoft Edge fails to properly secure private namespace. Successful exploitation could allow a local user to gain elevated privileges.

### **20627 - (MS16-119) Microsoft Edge Browser Privilege Escalation I (3192890)**

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

Risk Level: Medium  
CVE: CVE-2016-3388

#### Description

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

#### Observation

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

The flaw occurs when Microsoft Edge fails to properly secure private namespace. Successful exploitation could allow a local user to gain elevated privileges.

### **20629 - (MS16-119) Microsoft Edge Browser Credential Data Information Disclosure (3192890)**

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

Risk Level: Medium  
CVE: CVE-2016-3391

#### 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 Microsoft Browsers leave credential data in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

### **20630 - (MS16-119) Microsoft Edge Browser Information Disclosure I (3192890)**

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

Risk Level: Medium  
CVE: CVE-2016-3267

#### 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 Microsoft Edge does not properly handle objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

## **20639 - (MS16-121) Microsoft Office Memory Corruption Remote Code Execution (3194063)**

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

Risk Level: Medium

CVE: CVE-2016-7193

### 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 occurs when the Office software fails to properly handle objects in memory. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

## **20641 - (MS16-123) Microsoft Windows Win32k Privilege Escalation V (3192892)**

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

Risk Level: Medium

CVE: CVE-2016-3376

### 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 Windows kernel-mode driver fails to properly handle objects in memory. Successful exploitation could allow a local user to gain elevated privileges.

## **20642 - (MS16-123) Microsoft Windows Win32k Privilege Escalation IV (3192892)**

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

Risk Level: Medium

CVE: CVE-2016-7211

### 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 Windows kernel-mode driver fails to properly handle objects in memory. Successful exploitation could allow a local user to gain elevated privileges.

#### **20643 - (MS16-123) Microsoft Windows Win32k Privilege Escalation III (3192892)**

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

Risk Level: Medium

CVE: CVE-2016-7185

##### 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 Windows kernel-mode driver fails to properly handle objects in memory. Successful exploitation could allow a local user to gain elevated privileges.

#### **20644 - (MS16-123) Microsoft Windows Win32k Privilege Escalation II (3192892)**

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

Risk Level: Medium

CVE: CVE-2016-3241

##### 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 Windows kernel-mode driver fails to properly handle objects in memory. Successful exploitation could allow a local user to gain elevated privileges.

#### **20645 - (MS16-123) Microsoft Windows Win32k Privilege Escalation I (3192892)**

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

Risk Level: Medium

CVE: CVE-2016-3266

##### 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 Windows kernel-mode driver fails to properly handle objects in memory. Successful exploitation could allow

a local user to gain elevated privileges.

#### **20648 - (MS16-124) Microsoft Windows Kernel Privilege Escalation IV (3193227)**

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

Risk Level: Medium

CVE: CVE-2016-0079

##### Description

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

##### Observation

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

The flaw occurs when a Windows kernel API improperly allows a user to access sensitive registry information. Successful exploitation could allow a local user to gain elevated privileges.

#### **20649 - (MS16-124) Microsoft Windows Kernel Privilege Escalation III (3193227)**

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

Risk Level: Medium

CVE: CVE-2016-0075

##### Description

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

##### Observation

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

The flaw occurs when a Windows kernel API improperly allows a user to access sensitive registry information. Successful exploitation could allow a local user to gain elevated privileges.

#### **20650 - (MS16-124) Microsoft Windows Kernel Privilege Escalation II (3193227)**

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

Risk Level: Medium

CVE: CVE-2016-0073

##### Description

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

##### Observation

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

The flaw occurs when a Windows kernel API improperly allows a user to access sensitive registry information. Successful exploitation could allow a local user to gain elevated privileges.

## 20651 - (MS16-124) Microsoft Windows Kernel Privilege Escalation I (3193227)

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

Risk Level: Medium

CVE: CVE-2016-0070

### Description

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

### Observation

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

The flaw occurs when a Windows kernel API improperly allows a user to access sensitive registry information. Successful exploitation could allow a local user to gain elevated privileges.

## 20664 - (MS16-118) Microsoft Internet Explorer Information Disclosure I (3192887)

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

Risk Level: Medium

CVE: CVE-2016-3267

### 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 occurs when Microsoft Internet Explorer does not properly handle objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

## 20665 - (MS16-118) Microsoft Internet Explorer Information Disclosure III (3192887)

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

Risk Level: Medium

CVE: CVE-2016-3298

### 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 occurs when Microsoft Internet Explorer improperly handles objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

## 20671 - (MS16-118) Microsoft Internet Explorer Privilege Escalation I (3192887)

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

Risk Level: Medium  
CVE: CVE-2016-3387

#### Description

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

#### Observation

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

The flaw occurs when Microsoft Internet Explorer fails to properly secure private namespace. Successful exploitation could allow a local user to gain elevated privileges.

### **20672 - (MS16-118) Microsoft Internet Explorer Privilege Escalation II (3192887)**

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

Risk Level: Medium  
CVE: CVE-2016-3388

#### Description

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

#### Observation

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

The flaw occurs when Microsoft Internet Explorer fails to properly secure private namespace. Successful exploitation could allow a local user to gain elevated privileges.

### **20674 - (MS16-118) Microsoft Internet Explorer Information Disclosure II (3192887)**

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

Risk Level: Medium  
CVE: CVE-2016-3391

#### 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 occurs when Microsoft Internet Explorer leaves credential data in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

### **20676 - (MS16-125) Microsoft Windows Diagnostics Hub Privilege Escalation (3193229)**

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

Risk Level: Medium  
CVE: CVE-2016-7188

#### 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 the Windows Diagnostics Hub Standard Collector Service. Successful exploitation could allow a local user to gain elevated privileges.

### **20677 - (MS16-125) Security Update for Diagnostic Hub (3193229)**

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

Risk Level: Medium

CVE: CVE-2016-7188

### Description

A privilege escalation vulnerability is present in some versions of Microsoft Windows.

### Observation

Microsoft Windows is an industry standard operating system.

A privilege escalation vulnerability is present in some versions of Microsoft Windows. The flaw occurs in the Windows Diagnostics Hub Standard Collector Service. Successful exploitation could allow a local user to gain elevated privileges.

Microsoft has provided MS16-125 to address this issue. The host appears to be missing this patch.

### **20680 - (MS16-120) Microsoft Windows Graphics Win32k Privilege Escalation (3192884)**

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

Risk Level: Medium

CVE: CVE-2016-3270

### Description

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

### Observation

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

The flaw occurs when the Windows kernel fails to properly handle objects in memory. Successful exploitation could allow a local user to gain elevated privileges.

### **20682 - (MS16-120) Microsoft Windows Graphics GDI+ Information Disclosure III (3192884)**

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

Risk Level: Medium

CVE: CVE-2016-3263

### Description

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

### Observation

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

The flaw occurs in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

### **20683 - (MS16-120) Microsoft Windows Graphics GDI+ Information Disclosure II (3192884)**

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

Risk Level: Medium

CVE: CVE-2016-3262

### Description

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

### Observation

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

The flaw occurs in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

### **20684 - (MS16-120) Microsoft Windows Graphics GDI+ Information Disclosure I (3192884)**

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

Risk Level: Medium

CVE: CVE-2016-3209

### Description

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

### Observation

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

The flaw occurs in the way that the Windows Graphics Device Interface (GDI) handles objects in memory. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

### **20690 - (MS16-126) Internet Explorer Information Disclosure Vulnerability (3196067)**

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

Risk Level: Medium

CVE: CVE-2016-3298

### 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 the messaging API. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

### 20681 - (MS16-120) Microsoft Windows Graphics True Type Font Parsing Privilege Escalation (3192884)

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

Risk Level: Medium

CVE: CVE-2016-7182

#### Description

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

#### Observation

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

The flaw occurs when the Windows Graphics Component improperly handles objects in memory. Successful exploitation could allow a local user to gain elevated privileges.

### 20689 - (MS16-126) Security Update for Microsoft Internet Messaging API (3196067)

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

Risk Level: Medium

CVE: CVE-2016-3298

#### Description

A vulnerability is present in some versions of Microsoft Windows.

#### Observation

Microsoft Windows is an industry-standard operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw occurs when Inetres.dll and Inetcomm.dll fail to properly handle objects in memory. Successful exploitation could allow a remote attacker to obtain sensitive information.

Microsoft has provided MS16-126 to address these issues. The host appears to be missing this patch.

## 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.

### 6770 - (MS09-026) Microsoft Windows RPC Marshalling Engine Vulnerability (970238)

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

Risk Level: High

CVE: CVE-2009-0568

#### Update Details

Recommendation is updated

### **7223 - (MS09-062) Vulnerabilities In GDI+ Could Allow Remote Code Execution (957488)**

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

Risk Level: High

CVE: CVE-2009-2500, CVE-2009-2501, CVE-2009-2502, CVE-2009-2503, CVE-2009-2504, CVE-2009-2518, CVE-2009-2528, CVE-2009-3126

[Update Details](#)

Recommendation is updated

### **7332 - (MS09-065) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947)**

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

Risk Level: High

CVE: CVE-2009-1127, CVE-2009-2513, CVE-2009-2514

[Update Details](#)

Recommendation is updated

### **7545 - (MS09-026) Vulnerability In RPC Could Allow Elevation Of Privilege (970238)**

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

Risk Level: High

CVE: CVE-2009-0568

[Update Details](#)

Recommendation is updated

### **7736 - (MS08-026) Vulnerabilities In Microsoft Word Could Allow Remote Code Execution (951207)**

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

Risk Level: High

CVE: CVE-2008-1091, CVE-2008-1434

[Update Details](#)

Recommendation is updated

### **8529 - (MS10-020) Microsoft Windows SMB Client Memory Allocation Vulnerability (980232)**

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

Risk Level: High

CVE: CVE-2010-0269

[Update Details](#)

Recommendation is updated

### **8530 - (MS10-020) Microsoft Windows SMB Client Transaction Vulnerability (980232)**

---

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

Risk Level: High

CVE: CVE-2010-0270

Update Details

Recommendation is updated

**8531 - (MS10-020) Microsoft Windows SMB Client Response Parsing Vulnerability (980232)**

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

Risk Level: High

CVE: CVE-2010-0476

Update Details

Recommendation is updated

**8532 - (MS10-020) Microsoft Windows SMB Client Message Size Vulnerability (980232)**

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

Risk Level: High

CVE: CVE-2010-0477

Update Details

Recommendation is updated

**12206 - (MS11-043) Microsoft Windows SMB Client Could Allow Remote Code Execution (KB2536276)**

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

Risk Level: High

CVE: CVE-2011-1268

Update Details

Recommendation is updated

**12220 - (MS11-042) Microsoft Windows DFS Memory Corruption Remote Code Execution (2535512)**

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

Risk Level: High

CVE: CVE-2011-1868

Update Details

Recommendation is updated

**12229 - (MS11-043) Microsoft Windows SMB Client Could Allow Remote Code Execution (2536276)**

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

Risk Level: High  
CVE: CVE-2011-1268

[Update Details](#)

Recommendation is updated

**14377 - (MS12-075) Microsoft Windows Font Parsing Remote Code Execution (2761226)**

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

Risk Level: High  
CVE: CVE-2012-2897

[Update Details](#)

Recommendation is updated

**14381 - (MS12-075) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2761226)**

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

Risk Level: High  
CVE: CVE-2012-2530, CVE-2012-2553, CVE-2012-2897

[Update Details](#)

Recommendation is updated

**14495 - (MS12-078) Microsoft Windows True Type Font Parsing Remote Code Execution (2783534)**

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

Risk Level: High  
CVE: CVE-2012-4786

[Update Details](#)

Recommendation is updated

**14501 - (MS12-078) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2783534)**

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

Risk Level: High  
CVE: CVE-2012-2556, CVE-2012-4786

[Update Details](#)

Recommendation is updated

**14715 - (MS13-015) Microsoft .NET Framework WinForms Callback Privilege Escalation (2800277)**

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

Risk Level: High

CVE: CVE-2013-0073

[Update Details](#)

Recommendation is updated

**16694 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXI Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1804

[Update Details](#)

Recommendation is updated

**16710 - (MS14-035) Cumulative Security Update for Internet Explorer (2969262)**

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

Risk Level: High

CVE: CVE-2014-0282, CVE-2014-1762, CVE-2014-1764, CVE-2014-1766, CVE-2014-1769, CVE-2014-1770, CVE-2014-1771, CVE-2014-1772, CVE-2014-1773, CVE-2014-1774, CVE-2014-1775, CVE-2014-1777, CVE-2014-1778, CVE-2014-1779, CVE-2014-1780, CVE-2014-1781, CVE-2014-1782, CVE-2014-1783, CVE-2014-1784, CVE-2014-1785, CVE-2014-1786, CVE-2014-1788, CVE-2014-1789, CVE-2014-1790, CVE-2014-1791, CVE-2014-1792, CVE-2014-1794, CVE-2014-1795, CVE-2014-1796, CVE-2014-1797, CVE-2014-1799, CVE-2014-1800, CVE-2014-1802, CVE-2014-1803, CVE-2014-1804, CVE-2014-1805, CVE-2014-2753, CVE-2014-2754, CVE-2014-2755, CVE-2014-2756, CVE-2014-2757, CVE-2014-2758, CVE-2014-2759, CVE-2014-2760, CVE-2014-2761, CVE-2014-2763, CVE-2014-2764, CVE-2014-2765, CVE-2014-2766, CVE-2014-2767, CVE-2014-2768, CVE-2014-2769, CVE-2014-2770, CVE-2014-2771, CVE-2014-2772, CVE-2014-2773, CVE-2014-2775, CVE-2014-2776, CVE-2014-2777

[Update Details](#)

Recommendation is updated

**17100 - (MS14-052) Microsoft Internet Explorer Resource Anti-Malware Detection Information Disclosure (2977629)**

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

Risk Level: High

CVE: CVE-2013-7331

[Update Details](#)

Recommendation is updated

**17223 - (MS14-057) Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)**

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

Risk Level: High

CVE: CVE-2014-4073, CVE-2014-4121, CVE-2014-4122

[Update Details](#)

Recommendation is updated

### 17225 - (MS14-057) Microsoft .NET Framework Remote Code Execution (3000414)

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

Risk Level: High

CVE: CVE-2014-4121

#### Update Details

Recommendation is updated

### 17226 - (MS14-057) Microsoft .NET Framework ClickOnce Privilege Escalation (3000414)

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

Risk Level: High

CVE: CVE-2014-4073

#### Update Details

Recommendation is updated

### 18878 - (MS15-093) Security Update for Internet Explorer (3088903)

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

Risk Level: High

CVE: CVE-2015-2502

#### Update Details

Recommendation is updated

### 20140 - (MS16-077) Security Update for WPAD (3165191)

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

Risk Level: High

CVE: CVE-2016-3213, CVE-2016-3236

#### Update Details

Recommendation is updated

### 4907 - (MS07-014) Microsoft Word Malformed Function Vulnerability (929434)

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

Risk Level: High

CVE: CVE-2007-0515

#### Update Details

Recommendation is updated

### 5125 - (MS07-024) Microsoft Word Array Overflow (934232)



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

Risk Level: High

CVE: CVE-2007-0035, CVE-2007-0870, CVE-2007-1202

Update Details

Recommendation is updated

**5712 - (MS08-009) Microsoft Word Memory Corruption Vulnerability (947077)**

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

Risk Level: High

CVE: CVE-2008-0109

Update Details

Recommendation is updated

**5862 - (MS08-026) Microsoft Object Parsing Vulnerability (951207)**

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

Risk Level: High

CVE: CVE-2008-1091, CVE-2008-1434

Update Details

Recommendation is updated

**5863 - (MS08-026) Microsoft Word Cascading Style Sheet (CSS) Vulnerability (951207)**

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

Risk Level: High

CVE: CVE-2008-1091, CVE-2008-1434

Update Details

Recommendation is updated

**6105 - (MS08-052) Microsoft GDI+ VML Buffer Overrun Vulnerability (954593)**

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

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

**6106 - (MS08-052) Microsoft GDI+ EMF Memory Corruption Vulnerability (954593)**

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

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

**6107 - (MS08-052) Microsoft GDI+ GIF Parsing Vulnerability (954593)**

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

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

**6108 - (MS08-052) Microsoft GDI+WMF Buffer Overrun Vulnerability (954593)**

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

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

**6109 - (MS08-052) Microsoft GDI+ BMP Integer Overflow Vulnerability (954593)**

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

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

Update Details

Recommendation is updated

**6220 - (MS08-068) Microsoft SMB Credential Reflection Vulnerability (957097)**

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

Risk Level: High

CVE: CVE-2008-4037

Update Details

Recommendation is updated

**7211 - (MS09-062) GDI+ .Net PropertyItem Heap Overflow Vulnerability (957488)**

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

Risk Level: High

CVE: CVE-2009-2504

[Update Details](#)

Recommendation is updated

**7212 - (MS09-062) GDI+ PNG Heap Overflow Vulnerability (957488)**

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

Risk Level: High

CVE: CVE-2009-2501

[Update Details](#)

Recommendation is updated

**7213 - (MS09-062) GDI+ PNG Integer Overflow Vulnerability (957488)**

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

Risk Level: High

CVE: CVE-2009-3126

[Update Details](#)

Recommendation is updated

**7214 - (MS09-062) GDI+ TIFF Memory Corruption Vulnerability (957488)**

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

Risk Level: High

CVE: CVE-2009-2503

[Update Details](#)

Recommendation is updated

**7215 - (MS09-062) GDI+ TIFF Buffer Overflow Vulnerability (957488)**

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

Risk Level: High

CVE: CVE-2009-2502

[Update Details](#)

Recommendation is updated

**7216 - (MS09-062) GDI+ WMF Integer Overflow Vulnerability (957488)**

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

Risk Level: High

CVE: CVE-2009-2500

[Update Details](#)

Recommendation is updated

### **7217 - (MS09-062) Memory Corruption Vulnerability (957488)**

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

Risk Level: High

CVE: CVE-2009-2528

[Update Details](#)

Recommendation is updated

### **7218 - (MS09-062) Office BMP Integer Overflow Vulnerability (957488)**

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

Risk Level: High

CVE: CVE-2009-2518

[Update Details](#)

Recommendation is updated

### **7315 - (MS09-068) Vulnerability in Microsoft Office Word Allows Remote Code Execution (976307)**

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

Risk Level: High

CVE: CVE-2009-3135

[Update Details](#)

Recommendation is updated

### **7318 - (MS09-065) Win32k EOT Parsing Vulnerability (969947)**

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

Risk Level: High

CVE: CVE-2009-2514

[Update Details](#)

Recommendation is updated

### **7335 - (MS09-068) Vulnerability In Microsoft Office Word Could Allow Remote Code Execution (976307)**

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

Risk Level: High

CVE: CVE-2009-3135

[Update Details](#)

Recommendation is updated

### **7413 - (MS09-006) Vulnerabilities In Windows Kernel Could Allow Remote Code Execution (958690)**

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

Risk Level: High

CVE: CVE-2009-0081, CVE-2009-0082, CVE-2009-0083

#### Update Details

Recommendation is updated

### **7701 - (MS08-052) Vulnerabilities in GDI+ Could Allow Remote Code Execution (954593)**

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

Risk Level: High

CVE: CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015

#### Update Details

Recommendation is updated

### **7822 - (MS08-009) Vulnerability In Microsoft Word Could Allow Remote Code Execution (947077)**

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

Risk Level: High

CVE: CVE-2008-0109

#### Update Details

Recommendation is updated

### **7857 - (MS10-006) Microsoft Windows SMB Client Pool Corruption Vulnerability (978251)**

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

Risk Level: High

CVE: CVE-2010-0016

#### Update Details

Recommendation is updated

### **7858 - (MS10-006) Microsoft Windows SMB Client Race Condition Vulnerability (978251)**

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

Risk Level: High

CVE: CVE-2010-0017

#### Update Details

Recommendation is updated

### **7880 - (MS10-006) Vulnerabilities In SMB Client Could Allow Remote Code Execution (978251)**

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

Risk Level: High

CVE: CVE-2010-0016, CVE-2010-0017

Update Details

Recommendation is updated

**8154 - (MS08-068) Vulnerability In SMB Could Allow Remote Code Execution (957097)**

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

Risk Level: High

CVE: CVE-2008-4037

Update Details

Recommendation is updated

**8541 - (MS10-020) Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)**

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

Risk Level: High

CVE: CVE-2009-3676, CVE-2010-0269, CVE-2010-0270, CVE-2010-0476, CVE-2010-0477

Update Details

Recommendation is updated

**9066 - (MS10-036) Vulnerabilities In COM Validation In Microsoft Office Could Allow Remote Code Execution (983235)**

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

Risk Level: High

CVE: CVE-2010-1263

Update Details

Recommendation is updated

**9681 - (MS10-049) Microsoft Windows SChannel Malformed Certificate Request Remote Code Execution (980436)**

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

Risk Level: High

CVE: CVE-2010-2566

Update Details

Recommendation is updated

**9705 - (MS10-060) Microsoft Windows Microsoft Silverlight and Microsoft .NET Framework CLR Virtual Method Delegate Vulnerability (22659)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1898

[Update Details](#)

Recommendation is updated

#### **9706 - (MS10-060) Vulnerability in Microsoft Silverlight Could Allow Remote Code Execution (978464)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0019

[Update Details](#)

Recommendation is updated

#### **9707 - (MS10-056) Microsoft Office Word HTML Linked Objects Memory Corruption Vulnerability (2269638)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1903

[Update Details](#)

Recommendation is updated

#### **9708 - (MS10-056) Microsoft Office Word RTF Parsing Buffer Overflow Vulnerability (2269638)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1902

[Update Details](#)

Recommendation is updated

#### **9709 - (MS10-056) Microsoft Office Word RTF Parsing Engine Memory Corruption Vulnerability (2269638)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1901

[Update Details](#)

Recommendation is updated

#### **9710 - (MS10-056) Microsoft Office Word Record Parsing Vulnerability (2269638)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1900

[Update Details](#)

Recommendation is updated

**9713 - (MS10-049) Vulnerabilities in SChannel could allow Remote Code Execution (980436)**

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

Risk Level: High

CVE: CVE-2009-3555, CVE-2010-2566

[Update Details](#)

Recommendation is updated

**9724 - (MS10-060) Vulnerabilities In Microsoft Silverlight And .NET CLR Could Allow Remote Code Execution (2265906)**

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

Risk Level: High

CVE: CVE-2010-0019, CVE-2010-1898

[Update Details](#)

Recommendation is updated

**9725 - (MS10-056) Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (2269638)**

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

Risk Level: High

CVE: CVE-2010-1900, CVE-2010-1901, CVE-2010-1902, CVE-2010-1903

[Update Details](#)

Recommendation is updated

**10331 - (MS10-079) Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)**

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

Risk Level: High

CVE: CVE-2010-2747, CVE-2010-2748, CVE-2010-2750, CVE-2010-3214, CVE-2010-3215, CVE-2010-3216, CVE-2010-3217, CVE-2010-3218, CVE-2010-3219, CVE-2010-3220, CVE-2010-3221

[Update Details](#)

Recommendation is updated

**10332 - (MS10-079) Microsoft Office Word Uninitialized Pointer Remote Code Execution (2293194)**

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

Risk Level: High

CVE: CVE-2010-2747



[Update Details](#)

Recommendation is updated

**10333 - (MS10-079) Microsoft Office Word Boundary Check Remote Code Execution (2293194)**

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

Risk Level: High

CVE: CVE-2010-2748

[Update Details](#)

Recommendation is updated

**10334 - (MS10-079) Microsoft Office Word Index Remote Code Execution (2293194)**

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

Risk Level: High

CVE: CVE-2010-2750

[Update Details](#)

Recommendation is updated

**10335 - (MS10-079) Microsoft Office Word Stack Validation Remote Code Execution (2293194)**

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

Risk Level: High

CVE: CVE-2010-3214

[Update Details](#)

Recommendation is updated

**10336 - (MS10-079) Microsoft Office Word Return Value Remote Code Execution (2293194)**

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

Risk Level: High

CVE: CVE-2010-3215

[Update Details](#)

Recommendation is updated

**10337 - (MS10-079) Microsoft Office Word Bookmarks Remote Code Execution (2293194)**

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

Risk Level: High

CVE: CVE-2010-3216

[Update Details](#)

Recommendation is updated

#### **10338 - (MS10-079) Microsoft Office Word Pointer Remote Code Execution (2293194)**

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

Risk Level: High

CVE: CVE-2010-3217

[Update Details](#)

Recommendation is updated

#### **10339 - (MS10-079) Microsoft Office Word Heap Overflow Remote Code Execution (2293194)**

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

Risk Level: High

CVE: CVE-2010-3218

[Update Details](#)

Recommendation is updated

#### **10340 - (MS10-079) Microsoft Office Word Index Parsing Remote Code Execution (2293194)**

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

Risk Level: High

CVE: CVE-2010-3219

[Update Details](#)

Recommendation is updated

#### **10341 - (MS10-079) Microsoft Office Word Parsing Remote Code Execution (2293194)**

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

Risk Level: High

CVE: CVE-2010-3220

[Update Details](#)

Recommendation is updated

#### **10342 - (MS10-079) Microsoft Office Word Short Sign Remote Code Execution (2293194)**

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

Risk Level: High

CVE: CVE-2010-3221

[Update Details](#)

Recommendation is updated

### **11066 - (MS10-036) Microsoft Office COM Object Validation Vulnerability (983235)**

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

Risk Level: High

CVE: CVE-2010-1263

#### Update Details

Recommendation is updated

### **11340 - (MS11-022) Microsoft PowerPoint OfficeArt Atom RCE (2489283)**

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

Risk Level: High

CVE: CVE-2011-0976

#### Update Details

Recommendation is updated

### **11758 - (MS11-022) Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2489283)**

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

Risk Level: High

CVE: CVE-2011-0655, CVE-2011-0656, CVE-2011-0976

#### Update Details

Recommendation is updated

### **11765 - (MS11-029) Vulnerability in GDI+ Could Allow Remote Code Execution (2489979)**

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

Risk Level: High

CVE: CVE-2011-0041

#### Update Details

Recommendation is updated

### **11782 - (MS11-022) Microsoft PowerPoint Floating Point Techno-color Time Bandit RCE (2489283)**

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

Risk Level: High

CVE: CVE-2011-0655

#### Update Details

Recommendation is updated

### **11783 - (MS11-022) Microsoft PowerPoint Persist Directory RCE (2489283)**

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

Risk Level: High

CVE: CVE-2011-0656

Update Details

Recommendation is updated

**11785 - (MS11-029) Microsoft GDI+ Integer Overflow (2489979)**

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

Risk Level: High

CVE: CVE-2011-0041

Update Details

Recommendation is updated

**12219 - (MS11-041) Microsoft Windows Kernel-Mode Drivers Could Allow Remote Code Execution (KB2525694)**

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

Risk Level: High

CVE: CVE-2011-1873

Update Details

Recommendation is updated

**12228 - (MS11-039) Vulnerability In .NET Framework Could Allow Remote Code Execution (2514842)**

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

Risk Level: High

CVE: CVE-2011-0664

Update Details

Recommendation is updated

**12247 - (MS11-041) Vulnerability In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2525694)**

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

Risk Level: High

CVE: CVE-2011-1873

Update Details

Recommendation is updated

**12259 - (MS11-039) Microsoft Windows .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2514842)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0664

[Update Details](#)

Recommendation is updated

#### **12737 - (MS11-078) Microsoft .NET Framework Class Inheritance (2604930)**

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

Risk Level: High

CVE: CVE-2011-1253

[Update Details](#)

Recommendation is updated

#### **12740 - (MS11-077) Microsoft Windows Kernel-Mode Drivers Font Library File Buffer Overrun (2567053)**

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

Risk Level: High

CVE: CVE-2011-2003

[Update Details](#)

Recommendation is updated

#### **12744 - (MS11-077) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2567053)**

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

Risk Level: High

CVE: CVE-2011-1985, CVE-2011-2002, CVE-2011-2003, CVE-2011-2011

[Update Details](#)

Recommendation is updated

#### **12751 - (MS11-078) Vulnerability In .NET Framework And Microsoft Silverlight Could Allow Remote Code Execution (2604930)**

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

Risk Level: High

CVE: CVE-2011-1253

[Update Details](#)

Recommendation is updated

#### **12891 - (MS11-087) Microsoft Windows TrueType Font Parsing (2639417)**

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

Risk Level: High  
CVE: CVE-2011-3402

Update Details

Recommendation is updated

**13057 - (MS11-089) Microsoft Word Access Violation (2590602)**

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

Risk Level: High  
CVE: CVE-2011-1983

Update Details

Recommendation is updated

**13061 - (MS11-089) Vulnerabilities in Microsoft Word could allow for Remote Code Execution (2590602)**

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

Risk Level: High  
CVE: CVE-2011-1983

Update Details

Recommendation is updated

**13072 - (MS11-087) Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417)**

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

Risk Level: High  
CVE: CVE-2011-3402

Update Details

Recommendation is updated

**13121 - (MS12-008) Microsoft Windows GDI Access Violation (2660465)**

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

Risk Level: High  
CVE: CVE-2011-5046

Update Details

Recommendation is updated

**13183 - (MS12-004) Microsoft Media Player DirectShow Remote Code Execution (2636391)**

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

Risk Level: High  
CVE: CVE-2012-0004

[Update Details](#)

Recommendation is updated

**13185 - (MS12-004) Microsoft Media Player MIDI Remote Code Execution (2636391)**

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

Risk Level: High

CVE: CVE-2012-0003

[Update Details](#)

Recommendation is updated

**13186 - (MS12-004) Vulnerabilities In Windows Media Could Allow Remote Code Execution (2636391)**

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

Risk Level: High

CVE: CVE-2012-0003, CVE-2012-0004

[Update Details](#)

Recommendation is updated

**13188 - (MS12-001) Microsoft Windows Kernel SafeSEH Bypass (2644615)**

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

Risk Level: High

CVE: CVE-2012-0001

[Update Details](#)

Recommendation is updated

**13191 - (MS12-001) Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615)**

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

Risk Level: High

CVE: CVE-2012-0001

[Update Details](#)

Recommendation is updated

**13308 - (MS12-016) Microsoft .NET Framework Unmanaged Objects (2651026)**

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

Risk Level: High

CVE: CVE-2012-0014

[Update Details](#)

Recommendation is updated

### **13309 - (MS12-016) Microsoft .NET Framework Heap Corruption (2651026)**

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

Risk Level: High

CVE: CVE-2012-0015

#### Update Details

Recommendation is updated

### **13310 - (MS12-016) Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026)**

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

Risk Level: High

CVE: CVE-2012-0014, CVE-2012-0015

#### Update Details

Recommendation is updated

### **13617 - (MS12-029) Vulnerability in Microsoft Word Could Allow Remote Code Execution (2680352)**

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

Risk Level: High

CVE: CVE-2012-0183

#### Update Details

Recommendation is updated

### **13618 - (MS12-029) Microsoft Word RTF Mismatch Remote Code Execution (2680352)**

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

Risk Level: High

CVE: CVE-2012-0183

#### Update Details

Recommendation is updated

### **13622 - (MS12-034) Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)**

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

Risk Level: High

CVE: CVE-2011-3402, CVE-2012-0159, CVE-2012-0162, CVE-2012-0164, CVE-2012-0165, CVE-2012-0167, CVE-2012-0176, CVE-2012-0180, CVE-2012-0181, CVE-2012-1848

#### Update Details



Recommendation is updated

#### **13624 - (MS12-034) Microsoft Silverlight Double Free Remote Code Execution (2681578)**

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

Risk Level: High

CVE: CVE-2012-0176

[Update Details](#)

Recommendation is updated

#### **13625 - (MS12-034) Microsoft Windows .NET Buffer Allocation Remote Code Execution (2681578)**

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

Risk Level: High

CVE: CVE-2012-0162

[Update Details](#)

Recommendation is updated

#### **13629 - (MS12-034) Microsoft Windows GDI+ Heap Overflow Remote Code Execution (2681578)**

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

Risk Level: High

CVE: CVE-2012-0167

[Update Details](#)

Recommendation is updated

#### **13630 - (MS12-034) Microsoft Windows GDI+ Record Remote Code Execution (2681578)**

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

Risk Level: High

CVE: CVE-2012-0165

[Update Details](#)

Recommendation is updated

#### **13631 - (MS12-034) Microsoft Windows TrueType Font Parsing II (2681578)**

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

Risk Level: High

CVE: CVE-2012-0159

[Update Details](#)

Recommendation is updated

---

### 13632 - (MS12-034) Microsoft Windows TrueType Font Parsing (2681578)

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

Risk Level: High

CVE: CVE-2011-3402

#### Update Details

Recommendation is updated

### 13633 - (MS12-035) Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777)

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

Risk Level: High

CVE: CVE-2012-0160, CVE-2012-0161

#### Update Details

Recommendation is updated

### 13634 - (MS12-035) Microsoft Windows .NET Deserialization Remote Code Execution (2696777)

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

Risk Level: High

CVE: CVE-2012-0161

#### Update Details

Recommendation is updated

### 13635 - (MS12-035) Microsoft Windows .NET Serialization Remote Code Execution (2693777)

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

Risk Level: High

CVE: CVE-2012-0160

#### Update Details

Recommendation is updated

### 13782 - (MS12-039) Microsoft Lync Insecure Library Loading Remote Code Execution (2707956)

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

Risk Level: High

CVE: CVE-2012-1849

#### Update Details

Recommendation is updated

### 13784 - (MS12-039) Microsoft Windows TrueType Font Parsing II Remote Code Execution (2707956)

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

Risk Level: High

CVE: CVE-2012-0159

Update Details

Recommendation is updated

**13786 - (MS12-039) Microsoft Windows TrueType Font Parsing Remote Code Execution (2707956)**

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

Risk Level: High

CVE: CVE-2011-3402

Update Details

Recommendation is updated

**13788 - (MS12-039) Vulnerabilities in Lync Could Allow Remote Code Execution (2707956)**

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

Risk Level: High

CVE: CVE-2011-3402, CVE-2012-0159, CVE-2012-1849, CVE-2012-1858

Update Details

Recommendation is updated

**14014 - (MS12-055) Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2731847)**

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

Risk Level: High

CVE: CVE-2012-2527

Update Details

Recommendation is updated

**14207 - (MS12-064) Microsoft Word RTF Use After Free Remote Code Execution (2742319)**

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

Risk Level: High

CVE: CVE-2012-2528

Update Details

Recommendation is updated

**14208 - (MS12-064) Microsoft Word PAPX Section Corruption Remote Code Execution (2742319)**

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

Risk Level: High  
CVE: CVE-2012-0182

Update Details

Recommendation is updated

**14485 - (MS12-079) Microsoft Word Listoverridecount Remote Code Execution (2780642)**

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

Risk Level: High  
CVE: CVE-2012-2539

Update Details

Recommendation is updated

**14486 - (MS12-079) Vulnerability in Microsoft Word Could Allow Remote Code Execution (2780642)**

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

Risk Level: High  
CVE: CVE-2012-2539

Update Details

Recommendation is updated

**14494 - (MS12-078) Microsoft Windows Open Type Font Parsing Remote Code Execution (2783534)**

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

Risk Level: High  
CVE: CVE-2012-2556

Update Details

Recommendation is updated

**14648 - (MS13-019) Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (2790113)**

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

Risk Level: High  
CVE: CVE-2013-0076

Update Details

Recommendation is updated

**14671 - (MS13-009) Cumulative Security Update for Internet Explorer (2792100)**

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

Risk Level: High

CVE: CVE-2013-0015, CVE-2013-0018, CVE-2013-0019, CVE-2013-0020, CVE-2013-0021, CVE-2013-0022, CVE-2013-0023, CVE-2013-0024, CVE-2013-0025, CVE-2013-0026, CVE-2013-0027, CVE-2013-0028, CVE-2013-0029

Update Details

Recommendation is updated

**14695 - (MS13-009) Microsoft Internet Explorer CDispNode Use-After-Free Remote Code Execution (2792100)**

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

Risk Level: High

CVE: CVE-2013-0023

Update Details

Recommendation is updated

**14696 - (MS13-009) Microsoft Internet Explorer CHTML Use-After-Free Remote Code Execution (2792100)**

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

Risk Level: High

CVE: CVE-2013-0029

Update Details

Recommendation is updated

**14697 - (MS13-009) Microsoft Internet Explorer CMarkup Use-After-Free Remote Code Execution (2792100)**

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

Risk Level: High

CVE: CVE-2013-0020

Update Details

Recommendation is updated

**14698 - (MS13-009) Microsoft Internet Explorer CObjectElement Use-After-Free Remote Code Execution (2792100)**

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

Risk Level: High

CVE: CVE-2013-0028

Update Details

Recommendation is updated

**14699 - (MS13-009) Microsoft Internet Explorer CComWindowProxy Use-After-Free Remote Code Execution (2792100)**

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

Risk Level: High

CVE: CVE-2013-0019

[Update Details](#)

Recommendation is updated

**14700 - (MS13-009) Microsoft Internet Explorer CPasteCommand Use-After-Free Remote Code Execution (2792100)**

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

Risk Level: High

CVE: CVE-2013-0027

[Update Details](#)

Recommendation is updated

**14701 - (MS13-009) Microsoft Internet Explorer InsertElement Use-After-Free Remote Code Execution (2792100)**

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

Risk Level: High

CVE: CVE-2013-0026

[Update Details](#)

Recommendation is updated

**14702 - (MS13-009) Microsoft Internet Explorer LsGetTraillInfo Use-After-Free Remote Code Execution (2792100)**

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

Risk Level: High

CVE: CVE-2013-0022

[Update Details](#)

Recommendation is updated

**14703 - (MS13-009) Microsoft Internet Explorer PasteHTML Use-After-Free Remote Code Execution (2792100)**

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

Risk Level: High

CVE: CVE-2013-0024

[Update Details](#)

Recommendation is updated

**14704 - (MS13-009) Microsoft Internet Explorer SetCapture Use-After-Free Remote Code Execution (2792100)**

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

Risk Level: High

CVE: CVE-2013-0018

[Update Details](#)

Recommendation is updated

#### **14706 - (MS13-009) Microsoft Internet Explorer SLayoutRun Use-After-Free Remote Code Execution (2792100)**

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

Risk Level: High

CVE: CVE-2013-0025

[Update Details](#)

Recommendation is updated

#### **14707 - (MS13-009) Microsoft Internet Explorer Vtable Use-After-Free Remote Code Execution (2792100)**

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

Risk Level: High

CVE: CVE-2013-0021

[Update Details](#)

Recommendation is updated

#### **14713 - (MS13-015) Vulnerability in .NET Framework Could Allow Elevation of Privilege (2800277)**

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

Risk Level: High

CVE: CVE-2013-0073

[Update Details](#)

Recommendation is updated

#### **14719 - (MS13-017) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2799494)**

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

Risk Level: High

CVE: CVE-2013-1278, CVE-2013-1279, CVE-2013-1280

[Update Details](#)

Recommendation is updated

#### **14813 - (MS13-022) Critical Vulnerability In Silverlight Could Allow Remote Code Execution (2814124)**

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

Risk Level: High

CVE: CVE-2013-0074

[Update Details](#)

Recommendation is updated

---

### 14814 - (MS13-022) Microsoft Silverlight Double Dereference Remote Code Execution (2814124)

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

Risk Level: High

CVE: CVE-2013-0074

#### Update Details

Recommendation is updated

### 14928 - (MS13-036) Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege (2829996)

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

Risk Level: High

CVE: CVE-2013-1283, CVE-2013-1291, CVE-2013-1292, CVE-2013-1293

#### Update Details

Recommendation is updated

### 15052 - (MS13-041) Vulnerability in Lync Could Allow Remote Code Execution (2834695)

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

Risk Level: High

CVE: CVE-2013-1302

#### Update Details

Recommendation is updated

### 15053 - (MS13-041) Microsoft Office Lync Remote Code Execution (2834695)

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

Risk Level: High

CVE: CVE-2013-1302

#### Update Details

Recommendation is updated

### 15242 - (MS13-053) Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2850851)

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

Risk Level: High

CVE: CVE-2013-1300, CVE-2013-1340, CVE-2013-1345, CVE-2013-3129, CVE-2013-3167, CVE-2013-3172, CVE-2013-3173, CVE-2013-3660

#### Update Details

Recommendation is updated

### 15243 - (MS13-052) Microsoft Windows .NET Anonymous Method Injection Remote Code Execution (2861561)



---

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

Risk Level: High

CVE: CVE-2013-3133

[Update Details](#)

Recommendation is updated

#### **15244 - (MS13-052) Microsoft Windows .NET And Silverlight Array Access Remote Code Execution (2861561)**

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

Risk Level: High

CVE: CVE-2013-3131

[Update Details](#)

Recommendation is updated

#### **15245 - (MS13-052) Microsoft Windows .NET And Silverlight Array Allocation Remote Code Execution (2861561)**

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

Risk Level: High

CVE: CVE-2013-3134

[Update Details](#)

Recommendation is updated

#### **15247 - (MS13-052) Microsoft Windows .NET Delegate Reflection Remote Code Execution (2861561)**

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

Risk Level: High

CVE: CVE-2013-3132

[Update Details](#)

Recommendation is updated

#### **15248 - (MS13-052) Microsoft .NET Framework Delegate Serialization Remote Code Execution (2861561)**

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

Risk Level: High

CVE: CVE-2013-3171

[Update Details](#)

Recommendation is updated

#### **15249 - (MS13-052) Microsoft Windows Silverlight Null Pointer Remote Code Execution (2861561)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3178

[Update Details](#)

Recommendation is updated

#### **15250 - (MS13-052) Microsoft Windows .NET And Silverlight TrueType Font Parsing Remote Code Execution (2861561)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3129

[Update Details](#)

Recommendation is updated

#### **15252 - (MS13-052) Vulnerabilities In .NET Framework And Silverlight Could Allow Remote Code Execution (2861561)**

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3129, CVE-2013-3131, CVE-2013-3132, CVE-2013-3133, CVE-2013-3134, CVE-2013-3171, CVE-2013-3178

[Update Details](#)

Recommendation is updated

#### **15256 - (MS13-054) Microsoft Windows TrueType Font Parsing Remote Code Execution (2848295)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3129

[Update Details](#)

Recommendation is updated

#### **15258 - (MS13-053) Microsoft Windows Kernel Buffer Overwrite Remote Code Execution (2850851)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3173

[Update Details](#)

Recommendation is updated

#### **15259 - (MS13-053) Microsoft Windows Kernel Dereference Remote Code Execution (2850851)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1340

[Update Details](#)

Recommendation is updated

**15261 - (MS13-054) Vulnerability in GDI+ Could Allow Remote Code Execution (2848295)**

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

Risk Level: High

CVE: CVE-2013-3129

[Update Details](#)

Recommendation is updated

**15280 - (MS13-053) Microsoft Windows Kernel Memory Allocation Remote Code Execution (2850851)**

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

Risk Level: High

CVE: CVE-2013-1300

[Update Details](#)

Recommendation is updated

**15282 - (MS13-053) Microsoft Windows Kernel Remote Code Execution (2850851)**

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

Risk Level: High

CVE: CVE-2013-1345

[Update Details](#)

Recommendation is updated

**15283 - (MS13-053) Microsoft Windows Kernel TrueType Font Parsing Remote Code Execution (2850851)**

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

Risk Level: High

CVE: CVE-2013-3129

[Update Details](#)

Recommendation is updated

**15284 - (MS13-053) Microsoft Windows Win32k Information Disclosure (2850851)**

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

Risk Level: High

CVE: CVE-2013-3167

[Update Details](#)

Recommendation is updated

**15387 - (MS13-062) Microsoft Windows Remote Procedure Call Privilege Escalation (2849470)**

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

Risk Level: High

CVE: CVE-2013-3175

[Update Details](#)

Recommendation is updated

**15388 - (MS13-062) Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)**

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

Risk Level: High

CVE: CVE-2013-3175

[Update Details](#)

Recommendation is updated

**15535 - (MS13-072) Vulnerabilities In Microsoft Office Could Allow Remote Code Execution (2845537)**

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

Risk Level: High

CVE: CVE-2013-3160, CVE-2013-3847, CVE-2013-3848, CVE-2013-3849, CVE-2013-3850, CVE-2013-3851, CVE-2013-3852, CVE-2013-3853, CVE-2013-3854, CVE-2013-3855, CVE-2013-3856, CVE-2013-3857, CVE-2013-3858

[Update Details](#)

Recommendation is updated

**15537 - (MS13-069) Cumulative Security Update for Internet Explorer (2870699)**

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

Risk Level: High

CVE: CVE-2013-3201, CVE-2013-3202, CVE-2013-3203, CVE-2013-3204, CVE-2013-3205, CVE-2013-3206, CVE-2013-3207, CVE-2013-3208, CVE-2013-3209, CVE-2013-3845

[Update Details](#)

Recommendation is updated

**15540 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution I (2870699)**

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

Risk Level: High

CVE: CVE-2013-3201

[Update Details](#)

Recommendation is updated

**15545 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution II (2870699)**

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

Risk Level: High

CVE: CVE-2013-3202

[Update Details](#)

Recommendation is updated

**15546 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution III (2870699)**

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

Risk Level: High

CVE: CVE-2013-3203

[Update Details](#)

Recommendation is updated

**15547 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution IV (2870699)**

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

Risk Level: High

CVE: CVE-2013-3204

[Update Details](#)

Recommendation is updated

**15548 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution V (2870699)**

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

Risk Level: High

CVE: CVE-2013-3205

[Update Details](#)

Recommendation is updated

**15555 - (MS13-067) Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2834052)**

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

Risk Level: High

CVE: CVE-2013-0081, CVE-2013-1315, CVE-2013-1330, CVE-2013-3179, CVE-2013-3180, CVE-2013-3847, CVE-2013-3848, CVE-2013-3849, CVE-2013-3857, CVE-2013-3858

[Update Details](#)

Recommendation is updated

#### **15556 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution VI (2870699)**

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

Risk Level: High

CVE: CVE-2013-3206

[Update Details](#)

Recommendation is updated

#### **15558 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution VIII (2870699)**

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

Risk Level: High

CVE: CVE-2013-3208

[Update Details](#)

Recommendation is updated

#### **15562 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution IX (2870699)**

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

Risk Level: High

CVE: CVE-2013-3209

[Update Details](#)

Recommendation is updated

#### **15569 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution X (2870699)**

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

Risk Level: High

CVE: CVE-2013-3845

[Update Details](#)

Recommendation is updated

#### **15574 - (MS13-069) Microsoft Internet Explorer Memory Corruption Vulnerability Remote Code Execution VII (2870699)**

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

Risk Level: High

CVE: CVE-2013-3207

[Update Details](#)

Recommendation is updated

---

### 15720 - (MS13-080) Cumulative Security Update for Internet Explorer (2879017)

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

Risk Level: High

CVE: CVE-2013-3872, CVE-2013-3873, CVE-2013-3874, CVE-2013-3875, CVE-2013-3882, CVE-2013-3885, CVE-2013-3886, CVE-2013-3893, CVE-2013-3897

#### Update Details

Recommendation is updated

### 15721 - (MS13-084) Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2885089)

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

Risk Level: High

CVE: CVE-2013-3889, CVE-2013-3895

#### Update Details

Recommendation is updated

### 15726 - (MS13-086) Microsoft Word Memory Corruption I Remote Code Execution (2885084)

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

Risk Level: High

CVE: CVE-2013-3891

#### Update Details

Recommendation is updated

### 15727 - (MS13-086) Microsoft Word Memory Corruption II Remote Code Execution (2885084)

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

Risk Level: High

CVE: CVE-2013-3892

#### Update Details

Recommendation is updated

### 15728 - (MS13-082) Vulnerabilities In .NET Framework Could Allow Remote Code Execution (2878890)

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

Risk Level: High

CVE: CVE-2013-3128, CVE-2013-3860, CVE-2013-3861

#### Update Details

Recommendation is updated

### 15729 - (MS13-086) Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2885084)

---

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

Risk Level: High

CVE: CVE-2013-3891, CVE-2013-3892

[Update Details](#)

Recommendation is updated

#### **15734 - (MS13-081) Microsoft Windows TrueType Font CMAP Remote Code Execution (2870008)**

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

Risk Level: High

CVE: CVE-2013-3894

[Update Details](#)

Recommendation is updated

#### **15740 - (MS13-081) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2870008)**

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

Risk Level: High

CVE: CVE-2013-3128, CVE-2013-3200, CVE-2013-3879, CVE-2013-3880, CVE-2013-3881, CVE-2013-3888, CVE-2013-3894

[Update Details](#)

Recommendation is updated

#### **15751 - (MS13-081) Microsoft Windows Kernel-Mode Driver OpenType Font Parsing Remote Code Execution (2870008)**

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

Risk Level: High

CVE: CVE-2013-3128

[Update Details](#)

Recommendation is updated

#### **15910 - (MS13-090) Cumulative Security Update of ActiveX Kill Bits (2900986)**

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

Risk Level: High

CVE: CVE-2013-3918

[Update Details](#)

Recommendation is updated

#### **15911 - (MS13-090) Microsoft ActiveX KillBits InformationCardSignInHelper Remote Code Execution (2900986)**

Category: Windows Host Assessment -> Patches and Hotfixes



(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3918

[Update Details](#)

Recommendation is updated

#### **15928 - (MS13-088) Cumulative Security Update for Internet Explorer (2888505)**

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3871, CVE-2013-3908, CVE-2013-3909, CVE-2013-3910, CVE-2013-3911, CVE-2013-3912, CVE-2013-3914, CVE-2013-3915, CVE-2013-3916, CVE-2013-3917

[Update Details](#)

Recommendation is updated

#### **16013 - (MS13-096) Vulnerability In Microsoft Graphics Component Could Allow Remote Code Execution (2908005)**

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3906

[Update Details](#)

Recommendation is updated

#### **16019 - (MS13-097) Cumulative Security Update for Internet Explorer (2898785)**

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5045, CVE-2013-5046, CVE-2013-5047, CVE-2013-5048, CVE-2013-5049, CVE-2013-5051, CVE-2013-5052

[Update Details](#)

Recommendation is updated

#### **16020 - (MS13-097) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2898785)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5052

[Update Details](#)

Recommendation is updated

#### **16026 - (MS13-097) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2898785)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2013-5051

[Update Details](#)

Recommendation is updated

**16027 - (MS13-097) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2898785)**

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

Risk Level: High  
CVE: CVE-2013-5049

[Update Details](#)

Recommendation is updated

**16028 - (MS13-097) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2898785)**

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

Risk Level: High  
CVE: CVE-2013-5048

[Update Details](#)

Recommendation is updated

**16045 - (MS13-100) Microsoft Sharepoint Page Content Privilege Escalation (2904244)**

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

Risk Level: High  
CVE: CVE-2013-5059

[Update Details](#)

Recommendation is updated

**16214 - (MS14-001) Microsoft Word and Office Web Apps Remote Code Execution I (2916605)**

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

Risk Level: High  
CVE: CVE-2014-0258

[Update Details](#)

Recommendation is updated

**16215 - (MS14-001) Microsoft Word and Office Web Apps Remote Code Execution II (2916605)**

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

Risk Level: High  
CVE: CVE-2014-0259

[Update Details](#)

Recommendation is updated

**16216 - (MS14-001) Microsoft Word and Office Web Apps Remote Code Execution III (2916605)**

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

Risk Level: High

CVE: CVE-2014-0260

[Update Details](#)

Recommendation is updated

**16217 - (MS14-001) Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (2916605)**

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

Risk Level: High

CVE: CVE-2014-0258, CVE-2014-0259, CVE-2014-0260

[Update Details](#)

Recommendation is updated

**16288 - (MS14-010) Cumulative Security Update for Internet Explorer (2909921)**

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

Risk Level: High

CVE: CVE-2014-0267, CVE-2014-0268, CVE-2014-0269, CVE-2014-0270, CVE-2014-0271, CVE-2014-0272, CVE-2014-0273, CVE-2014-0274, CVE-2014-0275, CVE-2014-0276, CVE-2014-0277, CVE-2014-0278, CVE-2014-0279, CVE-2014-0280, CVE-2014-0281, CVE-2014-0283, CVE-2014-0284, CVE-2014-0285, CVE-2014-0286, CVE-2014-0287, CVE-2014-0288, CVE-2014-0289, CVE-2014-0290, CVE-2014-0293

[Update Details](#)

Recommendation is updated

**16289 - (MS14-010) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2909921)**

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

Risk Level: High

CVE: CVE-2014-0267

[Update Details](#)

Recommendation is updated

**16291 - (MS14-010) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2909921)**

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

Risk Level: High

CVE: CVE-2014-0269

[Update Details](#)

Recommendation is updated

**16292 - (MS14-010) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2909921)**

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

Risk Level: High

CVE: CVE-2014-0270

[Update Details](#)

Recommendation is updated

**16293 - (MS14-010) Microsoft Internet Explorer VBScript Remote Code Execution (2909921)**

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

Risk Level: High

CVE: CVE-2014-0271

[Update Details](#)

Recommendation is updated

**16294 - (MS14-010) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2909921)**

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

Risk Level: High

CVE: CVE-2014-0272

[Update Details](#)

Recommendation is updated

**16295 - (MS14-010) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2909921)**

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

Risk Level: High

CVE: CVE-2014-0273

[Update Details](#)

Recommendation is updated

**16296 - (MS14-010) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2909921)**

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

Risk Level: High

CVE: CVE-2014-0274

[Update Details](#)

Recommendation is updated

**16297 - (MS14-010) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2909921)**

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

Risk Level: High

CVE: CVE-2014-0275

[Update Details](#)

Recommendation is updated

**16298 - (MS14-010) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2909921)**

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

Risk Level: High

CVE: CVE-2014-0276

[Update Details](#)

Recommendation is updated

**16299 - (MS14-010) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2909921)**

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

Risk Level: High

CVE: CVE-2014-0277

[Update Details](#)

Recommendation is updated

**16300 - (MS14-010) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2909921)**

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

Risk Level: High

CVE: CVE-2014-0278

[Update Details](#)

Recommendation is updated

**16301 - (MS14-010) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2909921)**

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

Risk Level: High

CVE: CVE-2014-0279

[Update Details](#)

Recommendation is updated

### 16302 - (MS14-010) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0280

#### Update Details

Recommendation is updated

### 16304 - (MS14-010) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0283

#### Update Details

Recommendation is updated

### 16305 - (MS14-010) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0284

#### Update Details

Recommendation is updated

### 16306 - (MS14-010) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0285

#### Update Details

Recommendation is updated

### 16307 - (MS14-010) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0286

#### Update Details

Recommendation is updated

### 16308 - (MS14-010) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0287

#### Update Details

Recommendation is updated

### 16309 - (MS14-010) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0288

#### Update Details

Recommendation is updated

### 16310 - (MS14-010) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0289

#### Update Details

Recommendation is updated

### 16311 - (MS14-010) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (2909921)

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

Risk Level: High

CVE: CVE-2014-0290

#### Update Details

Recommendation is updated

### 16315 - (MS14-011) Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (2928390)

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

Risk Level: High

CVE: CVE-2014-0271

#### Update Details

Recommendation is updated

### 16316 - (MS14-011) Microsoft VBScript Memory Corruption Remote Code Execution (2928390)

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

Risk Level: High

CVE: CVE-2014-0271

Update Details

Recommendation is updated

**16317 - (MS14-009) Vulnerabilities In .NET Framework Could Allow Elevation Of Privilege (2916607)**

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

Risk Level: High

CVE: CVE-2014-0253, CVE-2014-0257, CVE-2014-0295

Update Details

Recommendation is updated

**16366 - (MS14-010) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2909921)**

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

Risk Level: High

CVE: CVE-2014-0281

Update Details

Recommendation is updated

**16405 - (MS14-012) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution(2925418)**

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

Risk Level: High

CVE: CVE-2014-0324

Update Details

Recommendation is updated

**16406 - (MS14-012) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution(2925418)**

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

Risk Level: High

CVE: CVE-2014-0322

Update Details

Recommendation is updated

**16407 - (MS14-012) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution(2925418)**

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



Risk Level: High  
CVE: CVE-2014-0321

[Update Details](#)

Recommendation is updated

**16408 - (MS14-012) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution(2925418)**

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

Risk Level: High  
CVE: CVE-2014-0314

[Update Details](#)

Recommendation is updated

**16409 - (MS14-012) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution(2925418)**

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

Risk Level: High  
CVE: CVE-2014-0313

[Update Details](#)

Recommendation is updated

**16410 - (MS14-012) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution(2925418)**

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

Risk Level: High  
CVE: CVE-2014-0312

[Update Details](#)

Recommendation is updated

**16411 - (MS14-012) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution(2925418)**

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

Risk Level: High  
CVE: CVE-2014-0311

[Update Details](#)

Recommendation is updated

**16412 - (MS14-012) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution(2925418)**

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

Risk Level: High  
CVE: CVE-2014-0309

[Update Details](#)

Recommendation is updated

**16413 - (MS14-012) Microsoft Internet Explorer Memory Corruption X Remote Code Execution(2925418)**

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

Risk Level: High

CVE: CVE-2014-0308

[Update Details](#)

Recommendation is updated

**16414 - (MS14-012) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution(2925418)**

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

Risk Level: High

CVE: CVE-2014-0307

[Update Details](#)

Recommendation is updated

**16415 - (MS14-012) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution(2925418)**

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

Risk Level: High

CVE: CVE-2014-0306

[Update Details](#)

Recommendation is updated

**16416 - (MS14-012) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution(2925418)**

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

Risk Level: High

CVE: CVE-2014-0305

[Update Details](#)

Recommendation is updated

**16417 - (MS14-012) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution(2925418)**

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

Risk Level: High

CVE: CVE-2014-0304

[Update Details](#)

Recommendation is updated

#### **16418 - (MS14-012) Microsoft Internet Explorer Memory Corruption V Remote Code Execution(2925418)**

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

Risk Level: High

CVE: CVE-2014-0303

[Update Details](#)

Recommendation is updated

#### **16419 - (MS14-012) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution(2925418)**

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

Risk Level: High

CVE: CVE-2014-0302

[Update Details](#)

Recommendation is updated

#### **16420 - (MS14-012) Microsoft Internet Explorer Memory Corruption III Remote Code Execution(2925418)**

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

Risk Level: High

CVE: CVE-2014-0299

[Update Details](#)

Recommendation is updated

#### **16421 - (MS14-012) Microsoft Internet Explorer Memory Corruption II Remote Code Execution(2925418)**

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

Risk Level: High

CVE: CVE-2014-0298

[Update Details](#)

Recommendation is updated

#### **16422 - (MS14-012) Microsoft Internet Explorer Memory Corruption I Remote Code Execution(2925418)**

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

Risk Level: High

CVE: CVE-2014-0297

[Update Details](#)

Recommendation is updated

### 16423 - (MS14-012) Cumulative Security Update for Internet Explorer (2925418)

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

Risk Level: High

CVE: CVE-2014-0297, CVE-2014-0298, CVE-2014-0299, CVE-2014-0302, CVE-2014-0303, CVE-2014-0304, CVE-2014-0305, CVE-2014-0306, CVE-2014-0307, CVE-2014-0308, CVE-2014-0309, CVE-2014-0311, CVE-2014-0312, CVE-2014-0313, CVE-2014-0314, CVE-2014-0321, CVE-2014-0322, CVE-2014-0324

[Update Details](#)

Recommendation is updated

### 16483 - (MS14-018) Cumulative Security Update for Internet Explorer (2950467)

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

Risk Level: High

CVE: CVE-2014-0325, CVE-2014-1751, CVE-2014-1752, CVE-2014-1753, CVE-2014-1755, CVE-2014-1760

[Update Details](#)

Recommendation is updated

### 16484 - (MS14-018) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2950467)

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

Risk Level: High

CVE: CVE-2014-0325, CVE-2014-3538

[Update Details](#)

Recommendation is updated

### 16485 - (MS14-018) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2950467)

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

Risk Level: High

CVE: CVE-2014-1751

[Update Details](#)

Recommendation is updated

### 16486 - (MS14-018) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2950467)

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

Risk Level: High

CVE: CVE-2014-1752

[Update Details](#)

Recommendation is updated

#### **16487 - (MS14-018) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2950467)**

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

Risk Level: High

CVE: CVE-2014-1753

##### Update Details

Recommendation is updated

#### **16488 - (MS14-018) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2950467)**

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

Risk Level: High

CVE: CVE-2014-1755

##### Update Details

Recommendation is updated

#### **16489 - (MS14-018) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2950467)**

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

Risk Level: High

CVE: CVE-2014-1760

##### Update Details

Recommendation is updated

#### **16492 - (MS14-017) Vulnerabilities In Microsoft Word And Office Web Apps Could Allow Remote Code Execution (2949660)**

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

Risk Level: High

CVE: CVE-2014-1757, CVE-2014-1758, CVE-2014-1761

##### Update Details

Recommendation is updated

#### **16493 - (MS14-017) Microsoft Word File Parsing Stack Overflow Remote Code Execution (2949660)**

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

Risk Level: High

CVE: CVE-2014-1758

##### Update Details

Recommendation is updated

#### **16494 - (MS14-017) Microsoft Word File Format Converter Remote Code Execution (2949660)**

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

Risk Level: High

CVE: CVE-2014-1757

Update Details

Recommendation is updated

**16495 - (MS14-017) Microsoft Word RTF Files Remote Code Execution (2949660)**

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

Risk Level: High

CVE: CVE-2014-1761

Update Details

Recommendation is updated

**16567 - (MS14-021) Microsoft Internet Explorer Use-After-Free VGX.DLL Remote Code Execution (2965111)**

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

Risk Level: High

CVE: CVE-2014-1776

Update Details

Recommendation is updated

**16594 - (MS14-022) Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (2952166)**

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

Risk Level: High

CVE: CVE-2014-0251, CVE-2014-1754, CVE-2014-1813

Update Details

Recommendation is updated

**16596 - (MS14-026) Microsoft .NET Framework TypeFilterLevel Remote Code Execution (2958732)**

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

Risk Level: High

CVE: CVE-2014-1806

Update Details

Recommendation is updated

**16597 - (MS14-022) Microsoft SharePoint Page Content Remote Code Execution (2952166)**

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

Risk Level: High  
CVE: CVE-2014-0251

[Update Details](#)

Recommendation is updated

**16598 - (MS14-022) Microsoft SharePoint XSS Remote Code Execution (2952166)**

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

Risk Level: High  
CVE: CVE-2014-1754

[Update Details](#)

Recommendation is updated

**16599 - (MS14-022) Microsoft Web Applications Page Content Remote Code Execution (2952166)**

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

Risk Level: High  
CVE: CVE-2014-1813

[Update Details](#)

Recommendation is updated

**16609 - (MS14-029) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2962482)**

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

Risk Level: High  
CVE: CVE-2014-0310

[Update Details](#)

Recommendation is updated

**16610 - (MS14-029) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2962482)**

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

Risk Level: High  
CVE: CVE-2014-1815

[Update Details](#)

Recommendation is updated

**16613 - (MS14-029) Cumulative Security Update for Internet Explorer (2962482)**

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

Risk Level: High  
CVE: CVE-2014-0310, CVE-2014-1815

[Update Details](#)

Recommendation is updated

**16690 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXVII Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1799

[Update Details](#)

Recommendation is updated

**16691 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXVIII Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1800

[Update Details](#)

Recommendation is updated

**16692 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXIX Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1802

[Update Details](#)

Recommendation is updated

**16693 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXX Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1803

[Update Details](#)

Recommendation is updated

**16695 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXII Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1805

[Update Details](#)



Recommendation is updated

#### **16696 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXIII Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-2753

[Update Details](#)

Recommendation is updated

#### **16697 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXIV Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-2754

[Update Details](#)

Recommendation is updated

#### **16698 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXV Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-2755

[Update Details](#)

Recommendation is updated

#### **16708 - (MS14-034) Vulnerability in Microsoft Word Could Allow Remote Code Execution (2969261)**

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

Risk Level: High

CVE: CVE-2014-2778

[Update Details](#)

Recommendation is updated

#### **16711 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXVI Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-2756

[Update Details](#)

Recommendation is updated

### 16712 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXVII Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-2757

#### Update Details

Recommendation is updated

### 16713 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXVIII Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-2758

#### Update Details

Recommendation is updated

### 16714 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXXIX Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-2759

#### Update Details

Recommendation is updated

### 16715 - (MS14-035) Microsoft Internet Explorer Memory Corruption XL Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-2760

#### Update Details

Recommendation is updated

### 16716 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLI Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-2761

#### Update Details

Recommendation is updated

### 16717 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLII Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-2763

Update Details

Recommendation is updated

**16718 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLIII Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-2764

Update Details

Recommendation is updated

**16719 - (MS14-036) Vulnerabilities In Microsoft Graphics Component Could Allow Remote Code Execution (2967487)**

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

Risk Level: High

CVE: CVE-2014-1817, CVE-2014-1818

Update Details

Recommendation is updated

**16720 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLIV Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-2765

Update Details

Recommendation is updated

**16721 - (MS14-036) Microsoft Unicode Scripts Processor Remote Code Execution (2967487)**

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

Risk Level: High

CVE: CVE-2014-1817

Update Details

Recommendation is updated

**16722 - (MS14-036) Microsoft GDI+ Image Parsing Remote Code Execution (2967487)**

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

Risk Level: High  
CVE: CVE-2014-1818

[Update Details](#)

Recommendation is updated

**16723 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLV Remote Code Execution (2969262)**

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

Risk Level: High  
CVE: CVE-2014-2766

[Update Details](#)

Recommendation is updated

**16724 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLVI Remote Code Execution (2969262)**

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

Risk Level: High  
CVE: CVE-2014-2767

[Update Details](#)

Recommendation is updated

**16725 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLVII Remote Code Execution (2969262)**

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

Risk Level: High  
CVE: CVE-2014-2768

[Update Details](#)

Recommendation is updated

**16726 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLVIII Remote Code Execution (2969262)**

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

Risk Level: High  
CVE: CVE-2014-2769

[Update Details](#)

Recommendation is updated

**16727 - (MS14-035) Microsoft Internet Explorer Memory Corruption XLIX Remote Code Execution (2969262)**

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

Risk Level: High  
CVE: CVE-2014-2770

[Update Details](#)

Recommendation is updated

**16728 - (MS14-035) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-0282

[Update Details](#)

Recommendation is updated

**16729 - (MS14-035) Microsoft Internet Explorer Memory Corruption L Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-2771

[Update Details](#)

Recommendation is updated

**16730 - (MS14-035) Microsoft Internet Explorer Memory Corruption LI Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-2772

[Update Details](#)

Recommendation is updated

**16731 - (MS14-035) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1762

[Update Details](#)

Recommendation is updated

**16732 - (MS14-035) Microsoft Internet Explorer Memory Corruption LII Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-2773

[Update Details](#)

Recommendation is updated

#### **16734 - (MS14-035) Microsoft Internet Explorer Memory Corruption LIV Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-2775

[Update Details](#)

Recommendation is updated

#### **16735 - (MS14-035) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1769

[Update Details](#)

Recommendation is updated

#### **16736 - (MS14-035) Microsoft Internet Explorer Memory Corruption LV Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-2776

[Update Details](#)

Recommendation is updated

#### **16737 - (MS14-035) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1766

[Update Details](#)

Recommendation is updated

#### **16739 - (MS14-035) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1770

[Update Details](#)

Recommendation is updated

#### 16740 - (MS14-035) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1772

##### Update Details

Recommendation is updated

#### 16741 - (MS14-035) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1773

##### Update Details

Recommendation is updated

#### 16742 - (MS14-035) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1774

##### Update Details

Recommendation is updated

#### 16743 - (MS14-035) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1775

##### Update Details

Recommendation is updated

#### 16746 - (MS14-035) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1779

##### Update Details

Recommendation is updated

#### 16747 - (MS14-035) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2969262)

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

Risk Level: High

CVE: CVE-2014-1780

Update Details

Recommendation is updated

**16748 - (MS14-035) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1781

Update Details

Recommendation is updated

**16749 - (MS14-035) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1782

Update Details

Recommendation is updated

**16750 - (MS14-035) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1783

Update Details

Recommendation is updated

**16751 - (MS14-035) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1784

Update Details

Recommendation is updated

**16752 - (MS14-035) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2969262)**

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



Risk Level: High  
CVE: CVE-2014-1785

[Update Details](#)

Recommendation is updated

**16753 - (MS14-035) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (2969262)**

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

Risk Level: High  
CVE: CVE-2014-1786

[Update Details](#)

Recommendation is updated

**16754 - (MS14-035) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (2969262)**

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

Risk Level: High  
CVE: CVE-2014-1788

[Update Details](#)

Recommendation is updated

**16755 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (2969262)**

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

Risk Level: High  
CVE: CVE-2014-1791

[Update Details](#)

Recommendation is updated

**16756 - (MS14-035) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (2969262)**

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

Risk Level: High  
CVE: CVE-2014-1790

[Update Details](#)

Recommendation is updated

**16757 - (MS14-035) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (2969262)**

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

Risk Level: High  
CVE: CVE-2014-1789

[Update Details](#)

Recommendation is updated

**16758 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXII Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1792

[Update Details](#)

Recommendation is updated

**16760 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXIV Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1795

[Update Details](#)

Recommendation is updated

**16761 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXIII Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1794

[Update Details](#)

Recommendation is updated

**16762 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXV Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1796

[Update Details](#)

Recommendation is updated

**16763 - (MS14-035) Microsoft Internet Explorer Memory Corruption XXVI Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-1797

[Update Details](#)

Recommendation is updated

#### **16796 - (MS14-035) Microsoft Internet Explorer Memory Corruption LVI Remote Code Execution (2969262)**

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

Risk Level: High

CVE: CVE-2014-2782

#### Update Details

Recommendation is updated

#### **16838 - (MS14-037) Cumulative Security Update for Internet Explorer (2975687)**

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

Risk Level: High

CVE: CVE-2014-1763, CVE-2014-1765, CVE-2014-2783, CVE-2014-2785, CVE-2014-2786, CVE-2014-2787, CVE-2014-2788, CVE-2014-2789, CVE-2014-2790, CVE-2014-2791, CVE-2014-2792, CVE-2014-2794, CVE-2014-2795, CVE-2014-2797, CVE-2014-2798, CVE-2014-2800, CVE-2014-2801, CVE-2014-2802, CVE-2014-2803, CVE-2014-2804, CVE-2014-2806, CVE-2014-2807, CVE-2014-2809, CVE-2014-2813

#### Update Details

Recommendation is updated

#### **16847 - (MS14-037) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2802

#### Update Details

Recommendation is updated

#### **16848 - (MS14-037) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2801

#### Update Details

Recommendation is updated

#### **16849 - (MS14-037) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2800

[Update Details](#)

Recommendation is updated

**16850 - (MS14-037) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2798

[Update Details](#)

Recommendation is updated

**16851 - (MS14-037) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2797

[Update Details](#)

Recommendation is updated

**16852 - (MS14-037) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2795

[Update Details](#)

Recommendation is updated

**16853 - (MS14-037) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2794

[Update Details](#)

Recommendation is updated

**16854 - (MS14-037) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2792

[Update Details](#)

Recommendation is updated

### **16855 - (MS14-037) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2791

#### Update Details

Recommendation is updated

### **16856 - (MS14-037) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2790

#### Update Details

Recommendation is updated

### **16857 - (MS14-037) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2789

#### Update Details

Recommendation is updated

### **16858 - (MS14-037) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2788

#### Update Details

Recommendation is updated

### **16859 - (MS14-037) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2787

#### Update Details

Recommendation is updated

### 16860 - (MS14-037) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2804

#### Update Details

Recommendation is updated

### 16863 - (MS14-037) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2806

#### Update Details

Recommendation is updated

### 16864 - (MS14-037) Microsoft Internet Explorer Memory Corruption XXII Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2807

#### Update Details

Recommendation is updated

### 16865 - (MS14-037) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2786

#### Update Details

Recommendation is updated

### 16866 - (MS14-037) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-2785

#### Update Details

Recommendation is updated

### 16867 - (MS14-037) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2975687)

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

Risk Level: High

CVE: CVE-2014-1765

Update Details

Recommendation is updated

**16868 - (MS14-037) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-1763

Update Details

Recommendation is updated

**16869 - (MS14-037) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2803

Update Details

Recommendation is updated

**16870 - (MS14-037) Microsoft Internet Explorer Memory Corruption XXIII Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2809

Update Details

Recommendation is updated

**16874 - (MS14-037) Microsoft Internet Explorer Memory Corruption XXIV Remote Code Execution (2975687)**

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

Risk Level: High

CVE: CVE-2014-2813

Update Details

Recommendation is updated

**16966 - (MS14-051) Cumulative Security Update for Internet Explorer (2976627)**

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

Risk Level: High

CVE: CVE-2014-2774, CVE-2014-2784, CVE-2014-2796, CVE-2014-2808, CVE-2014-2810, CVE-2014-2811, CVE-2014-2817, CVE-2014-2818, CVE-2014-2819, CVE-2014-2820, CVE-2014-2821, CVE-2014-2822, CVE-2014-2823, CVE-2014-2824, CVE-2014-2825, CVE-2014-2826, CVE-2014-2827, CVE-2014-4050, CVE-2014-4051, CVE-2014-4052, CVE-2014-4055, CVE-2014-4056, CVE-2014-4057, CVE-2014-4058, CVE-2014-4063, CVE-2014-4067

Update Details

Recommendation is updated

**16967 - (MS14-051) Microsoft Internet Explorer Memory Corruption XXVIII Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-4067

Update Details

Recommendation is updated

**16968 - (MS14-051) Microsoft Internet Explorer Memory Corruption XXVII Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-2827

Update Details

Recommendation is updated

**16971 - (MS14-051) Microsoft Internet Explorer Memory Corruption XXV Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-2822

Update Details

Recommendation is updated

**16972 - (MS14-051) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-2821

Update Details

Recommendation is updated

**16973 - (MS14-051) Microsoft Internet Explorer Memory Corruption XXIII Remote Code Execution (2976627)**

Category: Windows Host Assessment -> Patches and Hotfixes



(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4063

[Update Details](#)

Recommendation is updated

#### **16974 - (MS14-051) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2976627)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2820

[Update Details](#)

Recommendation is updated

#### **16975 - (MS14-051) Microsoft Internet Explorer Memory Corruption XXII Remote Code Execution (2976627)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4058

[Update Details](#)

Recommendation is updated

#### **16976 - (MS14-051) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (2976627)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4057

[Update Details](#)

Recommendation is updated

#### **16977 - (MS14-051) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (2976627)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-4056

[Update Details](#)

Recommendation is updated

#### **16978 - (MS14-051) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2976627)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-2818

[Update Details](#)

Recommendation is updated

**16979 - (MS14-051) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-4055

[Update Details](#)

Recommendation is updated

**16980 - (MS14-051) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-4052

[Update Details](#)

Recommendation is updated

**16981 - (MS14-051) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-4051

[Update Details](#)

Recommendation is updated

**16982 - (MS14-051) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-4050

[Update Details](#)

Recommendation is updated

**16983 - (MS14-051) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-2826

[Update Details](#)

Recommendation is updated

**16984 - (MS14-051) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-2811

[Update Details](#)

Recommendation is updated

**16985 - (MS14-051) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-2825

[Update Details](#)

Recommendation is updated

**16986 - (MS14-051) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-2810

[Update Details](#)

Recommendation is updated

**16987 - (MS14-051) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-2824

[Update Details](#)

Recommendation is updated

**16988 - (MS14-051) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-2808

[Update Details](#)

Recommendation is updated

#### **16989 - (MS14-051) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-2796

[Update Details](#)

Recommendation is updated

#### **16990 - (MS14-051) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-2784

[Update Details](#)

Recommendation is updated

#### **16991 - (MS14-051) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-2823

[Update Details](#)

Recommendation is updated

#### **16992 - (MS14-051) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2976627)**

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

Risk Level: High

CVE: CVE-2014-2774

[Update Details](#)

Recommendation is updated

#### **17064 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXVI Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4111

[Update Details](#)

Recommendation is updated

---

### 17065 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXV Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4110

#### Update Details

Recommendation is updated

### 17066 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXIV Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4109

#### Update Details

Recommendation is updated

### 17067 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXIII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4108

#### Update Details

Recommendation is updated

### 17068 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4107

#### Update Details

Recommendation is updated

### 17069 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXXI Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4106

#### Update Details

Recommendation is updated

### 17070 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXX Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4105

Update Details

Recommendation is updated

**17071 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXIX Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4104

Update Details

Recommendation is updated

**17072 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXVIII Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4103

Update Details

Recommendation is updated

**17073 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXVII Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4102

Update Details

Recommendation is updated

**17074 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXVI Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4101

Update Details

Recommendation is updated

**17075 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXV Remote Code Execution (2977629)**

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

Risk Level: High  
CVE: CVE-2014-4100

Update Details

Recommendation is updated

**17076 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXIV Remote Code Execution (2977629)**

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

Risk Level: High  
CVE: CVE-2014-4099

Update Details

Recommendation is updated

**17077 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXIII Remote Code Execution (2977629)**

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

Risk Level: High  
CVE: CVE-2014-4098

Update Details

Recommendation is updated

**17078 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXII Remote Code Execution (2977629)**

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

Risk Level: High  
CVE: CVE-2014-4097

Update Details

Recommendation is updated

**17079 - (MS14-052) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (2977629)**

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

Risk Level: High  
CVE: CVE-2014-4096

Update Details

Recommendation is updated

**17080 - (MS14-052) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (2977629)**

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

Risk Level: High  
CVE: CVE-2014-4095

[Update Details](#)

Recommendation is updated

**17081 - (MS14-052) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4094

[Update Details](#)

Recommendation is updated

**17082 - (MS14-052) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4093

[Update Details](#)

Recommendation is updated

**17083 - (MS14-052) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4092

[Update Details](#)

Recommendation is updated

**17084 - (MS14-052) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4091

[Update Details](#)

Recommendation is updated

**17085 - (MS14-052) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4090

[Update Details](#)



Recommendation is updated

#### **17086 - (MS14-052) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4089

[Update Details](#)

Recommendation is updated

#### **17087 - (MS14-052) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4088

[Update Details](#)

Recommendation is updated

#### **17088 - (MS14-052) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4087

[Update Details](#)

Recommendation is updated

#### **17089 - (MS14-052) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4086

[Update Details](#)

Recommendation is updated

#### **17090 - (MS14-052) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4085

[Update Details](#)

Recommendation is updated

### 17091 - (MS14-052) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4084

#### Update Details

Recommendation is updated

### 17092 - (MS14-052) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4083

#### Update Details

Recommendation is updated

### 17093 - (MS14-052) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4082

#### Update Details

Recommendation is updated

### 17094 - (MS14-052) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4081

#### Update Details

Recommendation is updated

### 17095 - (MS14-052) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4080

#### Update Details

Recommendation is updated

### 17096 - (MS14-052) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2977629)

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

Risk Level: High

CVE: CVE-2014-4079

[Update Details](#)

Recommendation is updated

**17097 - (MS14-052) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4065

[Update Details](#)

Recommendation is updated

**17098 - (MS14-052) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-4059

[Update Details](#)

Recommendation is updated

**17099 - (MS14-052) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2977629)**

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

Risk Level: High

CVE: CVE-2014-2799

[Update Details](#)

Recommendation is updated

**17101 - (MS14-052) Cumulative Security Update for Internet Explorer (2977629)**

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

Risk Level: High

CVE: CVE-2013-7331, CVE-2014-4082, CVE-2014-4083, CVE-2014-4084, CVE-2014-4085, CVE-2014-4086, CVE-2014-4087, CVE-2014-4088, CVE-2014-4089, CVE-2014-4090, CVE-2014-4091, CVE-2014-4092, CVE-2014-4093, CVE-2014-4094, CVE-2014-4095, CVE-2014-4096, CVE-2014-4097, CVE-2014-4098, CVE-2014-4099, CVE-2014-4100, CVE-2014-4101, CVE-2014-4102, CVE-2014-4103, CVE-2014-4104, CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109, CVE-2014-4110, CVE-2014-4111

[Update Details](#)

Recommendation is updated

### 17227 - (MS14-058) Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061)

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

Risk Level: High

CVE: CVE-2014-4113, CVE-2014-4148

#### Update Details

Recommendation is updated

### 17228 - (MS14-058) Microsoft Windows Win32k.sys Privilege Escalation (3000061)

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

Risk Level: High

CVE: CVE-2014-4113

#### Update Details

Recommendation is updated

### 17231 - (MS14-056) Cumulative Security Update for Internet Explorer (2987107)

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

Risk Level: High

CVE: CVE-2014-4123, CVE-2014-4124, CVE-2014-4126, CVE-2014-4127, CVE-2014-4128, CVE-2014-4129, CVE-2014-4130, CVE-2014-4132, CVE-2014-4133, CVE-2014-4134, CVE-2014-4137, CVE-2014-4138, CVE-2014-4140, CVE-2014-4141

#### Update Details

Recommendation is updated

### 17235 - (MS14-056) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2987107)

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

Risk Level: High

CVE: CVE-2014-4126

#### Update Details

Recommendation is updated

### 17236 - (MS14-056) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2987107)

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

Risk Level: High

CVE: CVE-2014-4127

#### Update Details

Recommendation is updated

### 17237 - (MS14-056) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2987107)

---

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

Risk Level: High

CVE: CVE-2014-4128

Update Details

Recommendation is updated

**17238 - (MS14-056) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2987107)**

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

Risk Level: High

CVE: CVE-2014-4132

Update Details

Recommendation is updated

**17239 - (MS14-056) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2987107)**

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

Risk Level: High

CVE: CVE-2014-4129

Update Details

Recommendation is updated

**17240 - (MS14-056) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2987107)**

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

Risk Level: High

CVE: CVE-2014-4130

Update Details

Recommendation is updated

**17241 - (MS14-056) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2987107)**

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

Risk Level: High

CVE: CVE-2014-4133

Update Details

Recommendation is updated

**17242 - (MS14-056) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2987107)**

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

Risk Level: High  
CVE: CVE-2014-4134

Update Details

Recommendation is updated

**17243 - (MS14-056) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2987107)**

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

Risk Level: High  
CVE: CVE-2014-4137

Update Details

Recommendation is updated

**17244 - (MS14-056) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2987107)**

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

Risk Level: High  
CVE: CVE-2014-4138

Update Details

Recommendation is updated

**17245 - (MS14-056) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (2987107)**

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

Risk Level: High  
CVE: CVE-2014-4141

Update Details

Recommendation is updated

**17250 - (MS14-058) Microsoft Windows TrueType Font Parsing Remote Code Execution (3000061)**

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

Risk Level: High  
CVE: CVE-2014-4148

Update Details

Recommendation is updated

**17257 - (MS14-061) Vulnerability in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3000434)**

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

Risk Level: High

CVE: CVE-2014-4117

[Update Details](#)

Recommendation is updated

**17258 - (MS14-061) Microsoft Word File Format Remote Code Execution (3000434)**

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

Risk Level: High

CVE: CVE-2014-4117

[Update Details](#)

Recommendation is updated

**17259 - (MS14-061) Vulnerability in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3000434)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-4117

[Update Details](#)

Recommendation is updated

**17372 - (MS14-065) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3003057)**

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

Risk Level: High

CVE: CVE-2014-4143

[Update Details](#)

Recommendation is updated

**17373 - (MS14-065) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3003057)**

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

Risk Level: High

CVE: CVE-2014-6337

[Update Details](#)

Recommendation is updated

**17374 - (MS14-065) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3003057)**

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

Risk Level: High

CVE: CVE-2014-6341

[Update Details](#)

Recommendation is updated

#### **17375 - (MS14-065) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3003057)**

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

Risk Level: High

CVE: CVE-2014-6342

[Update Details](#)

Recommendation is updated

#### **17376 - (MS14-065) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (3003057)**

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

Risk Level: High

CVE: CVE-2014-6343

[Update Details](#)

Recommendation is updated

#### **17377 - (MS14-065) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3003057)**

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

Risk Level: High

CVE: CVE-2014-6344

[Update Details](#)

Recommendation is updated

#### **17378 - (MS14-065) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3003057)**

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

Risk Level: High

CVE: CVE-2014-6347

[Update Details](#)

Recommendation is updated

#### **17379 - (MS14-065) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3003057)**

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

Risk Level: High

CVE: CVE-2014-6348

[Update Details](#)

Recommendation is updated



### 17380 - (MS14-065) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6351

#### Update Details

Recommendation is updated

### 17381 - (MS14-065) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3003057)

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

Risk Level: High

CVE: CVE-2014-6353

#### Update Details

Recommendation is updated

### 17384 - (MS14-065) Cumulative Security Update for Internet Explorer (3003057)

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

Risk Level: High

CVE: CVE-2014-4143, CVE-2014-6323, CVE-2014-6337, CVE-2014-6339, CVE-2014-6340, CVE-2014-6341, CVE-2014-6342, CVE-2014-6343, CVE-2014-6344, CVE-2014-6345, CVE-2014-6346, CVE-2014-6347, CVE-2014-6348, CVE-2014-6349, CVE-2014-6350, CVE-2014-6351, CVE-2014-6353

#### Update Details

Recommendation is updated

### 17385 - (MS14-069) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3009710)

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

Risk Level: High

CVE: CVE-2014-6333 , CVE-2014-6334 , CVE-2014-6335

#### Update Details

Recommendation is updated

### 17386 - (MS14-069) Microsoft Word Invalid Pointer Remote Code Execution (3009710)

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

Risk Level: High

CVE: CVE-2014-6335

#### Update Details

Recommendation is updated

### 17387 - (MS14-069) Microsoft Word Bad Index Remote Code Execution (3009710)

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

Risk Level: High

CVE: CVE-2014-6334

#### Update Details

Recommendation is updated

### 17388 - (MS14-069) Microsoft Word Double Delete Remote Code Execution (3009710)

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

Risk Level: High

CVE: CVE-2014-6333

#### Update Details

Recommendation is updated

### 17395 - (MS14-072) Vulnerability in .NET Framework Could Allow Elevation of Privilege (3005210)

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

Risk Level: High

CVE: CVE-2014-4149

#### Update Details

Recommendation is updated

### 17396 - (MS14-072) Microsoft .NET Framework Remoting TypeFilterLevel Privilege Escalation (3005210)

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

Risk Level: High

CVE: CVE-2014-4149

#### Update Details

Recommendation is updated

### 17485 - (MS14-081) Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow Remote Code Execution (3017301)

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

Risk Level: High

CVE: CVE-2014-6356 , CVE-2014-6357

#### Update Details

Recommendation is updated

### 17486 - (MS14-081) Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow Remote Code Execution

**(3017301)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2014-6356 , CVE-2014-6357

Update Details

Recommendation is updated

**17488 - (MS14-081) Microsoft Word Index Remote Code Execution (3017301)**

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

Risk Level: High

CVE: CVE-2014-6356

Update Details

Recommendation is updated

**17489 - (MS14-081) Microsoft Word Use-After-Free Remote Code Execution (3017301)**

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

Risk Level: High

CVE: CVE-2014-6357

Update Details

Recommendation is updated

**17498 - (MS14-080) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3008923)**

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

Risk Level: High

CVE: CVE-2014-6327

Update Details

Recommendation is updated

**17499 - (MS14-080) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3008923)**

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

Risk Level: High

CVE: CVE-2014-6329

Update Details

Recommendation is updated

**17500 - (MS14-080) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3008923)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6330

[Update Details](#)

Recommendation is updated

#### **17501 - (MS14-080) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3008923)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6366

[Update Details](#)

Recommendation is updated

#### **17502 - (MS14-080) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (3008923)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6369

[Update Details](#)

Recommendation is updated

#### **17503 - (MS14-080) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3008923)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6373

[Update Details](#)

Recommendation is updated

#### **17504 - (MS14-080) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3008923)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6374

[Update Details](#)

Recommendation is updated

#### **17505 - (MS14-080) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3008923)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6375

[Update Details](#)

Recommendation is updated

**17506 - (MS14-080) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3008923)**

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

Risk Level: High

CVE: CVE-2014-6376

[Update Details](#)

Recommendation is updated

**17507 - (MS14-080) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3008923)**

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

Risk Level: High

CVE: CVE-2014-8966

[Update Details](#)

Recommendation is updated

**17508 - (MS14-080) Microsoft Internet Explorer VBScript Memory Corruption Remote Code Execution (3008923)**

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

Risk Level: High

CVE: CVE-2014-6363

[Update Details](#)

Recommendation is updated

**17512 - (MS14-080) Cumulative Security Update for Internet Explorer (3008923)**

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

Risk Level: High

CVE: CVE-2014-6327, CVE-2014-6328, CVE-2014-6329, CVE-2014-6330, CVE-2014-6363, CVE-2014-6365, CVE-2014-6366, CVE-2014-6368, CVE-2014-6369, CVE-2014-6373, CVE-2014-6374, CVE-2014-6375, CVE-2014-6376, CVE-2014-8966

[Update Details](#)

Recommendation is updated

**17795 - (MS15-009) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0017

[Update Details](#)

Recommendation is updated

**17796 - (MS15-009) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0018

[Update Details](#)

Recommendation is updated

**17797 - (MS15-009) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0019

[Update Details](#)

Recommendation is updated

**17798 - (MS15-009) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0020

[Update Details](#)

Recommendation is updated

**17799 - (MS15-009) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0021

[Update Details](#)

Recommendation is updated

**17800 - (MS15-009) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0022

[Update Details](#)

Recommendation is updated

#### **17801 - (MS15-009) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0023

[Update Details](#)

Recommendation is updated

#### **17802 - (MS15-009) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0025

[Update Details](#)

Recommendation is updated

#### **17803 - (MS15-009) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0026

[Update Details](#)

Recommendation is updated

#### **17804 - (MS15-009) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0027

[Update Details](#)

Recommendation is updated

#### **17805 - (MS15-009) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0028

[Update Details](#)

Recommendation is updated

### 17806 - (MS15-009) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0029

#### Update Details

Recommendation is updated

### 17807 - (MS15-009) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0030

#### Update Details

Recommendation is updated

### 17808 - (MS15-009) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0031

#### Update Details

Recommendation is updated

### 17809 - (MS15-009) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0035

#### Update Details

Recommendation is updated

### 17810 - (MS15-009) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (3034682)

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

Risk Level: High

CVE: CVE-2015-0036

#### Update Details

Recommendation is updated

### 17811 - (MS15-009) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (3034682)



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

Risk Level: High

CVE: CVE-2015-0037

Update Details

Recommendation is updated

**17812 - (MS15-009) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0038

Update Details

Recommendation is updated

**17813 - (MS15-009) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0039

Update Details

Recommendation is updated

**17814 - (MS15-009) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0040

Update Details

Recommendation is updated

**17815 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0041

Update Details

Recommendation is updated

**17818 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXIV Remote Code Execution (3034682)**

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

Risk Level: High  
CVE: CVE-2015-0044

[Update Details](#)

Recommendation is updated

**17819 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXV Remote Code Execution (3034682)**

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

Risk Level: High  
CVE: CVE-2015-0045

[Update Details](#)

Recommendation is updated

**17820 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXVI Remote Code Execution (3034682)**

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

Risk Level: High  
CVE: CVE-2015-0046

[Update Details](#)

Recommendation is updated

**17821 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXVII Remote Code Execution (3034682)**

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

Risk Level: High  
CVE: CVE-2015-0048

[Update Details](#)

Recommendation is updated

**17822 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXVIII Remote Code Execution (3034682)**

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

Risk Level: High  
CVE: CVE-2015-0049

[Update Details](#)

Recommendation is updated

**17823 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXIX Remote Code Execution (3034682)**

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

Risk Level: High  
CVE: CVE-2015-0050

[Update Details](#)

Recommendation is updated

**17825 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXX Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0052

[Update Details](#)

Recommendation is updated

**17826 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXXI Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0053

[Update Details](#)

Recommendation is updated

**17829 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXXII Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0066

[Update Details](#)

Recommendation is updated

**17830 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXXIII Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0067

[Update Details](#)

Recommendation is updated

**17831 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXXIV Remote Code Execution (3034682)**

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

Risk Level: High

CVE: CVE-2015-0068

[Update Details](#)

Recommendation is updated

#### **17838 - (MS15-012) Vulnerability in Microsoft Office Could Allow Remote Code Execution (3032328)**

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

Risk Level: High

CVE: CVE-2015-0063, CVE-2015-0064, CVE-2015-0065

[Update Details](#)

Recommendation is updated

#### **17839 - (MS15-012) Microsoft Word OneTableDocumentStream Remote Code Execution (3032328)**

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

Risk Level: High

CVE: CVE-2015-0065

[Update Details](#)

Recommendation is updated

#### **17840 - (MS15-012) Microsoft Office Remote Code Execution (3032328)**

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

Risk Level: High

CVE: CVE-2015-0064

[Update Details](#)

Recommendation is updated

#### **17841 - (MS15-012) Microsoft Excel Remote Code Execution (3032328)**

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

Risk Level: High

CVE: CVE-2015-0063

[Update Details](#)

Recommendation is updated

#### **17854 - (MS15-010) Microsoft Windows TrueType Font Parsing Remote Code Execution (3036220)**

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

Risk Level: High

CVE: CVE-2015-0059

[Update Details](#)

Recommendation is updated

### **17974 - (MS15-022) Vulnerabilities in Microsoft Office could allow Elevation of Privilege (3038999)**

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

Risk Level: High

CVE: CVE-2015-0085, CVE-2015-0086, CVE-2015-0097, CVE-2015-1633, CVE-2015-1636

#### Update Details

Recommendation is updated

### **17977 - (MS15-020) Microsoft Windows Shell DLL Planting Remote Code Execution (3041836)**

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

Risk Level: High

CVE: CVE-2015-0096

#### Update Details

Recommendation is updated

### **17978 - (MS15-020) Microsoft Windows Shell WTS Remote Code Execution (3041836)**

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

Risk Level: High

CVE: CVE-2015-0081

#### Update Details

Recommendation is updated

### **17987 - (MS15-022) Microsoft Office RTF Handling Remote Code Execution (3038999)**

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

Risk Level: High

CVE: CVE-2015-0086

#### Update Details

Recommendation is updated

### **18005 - (MS15-020) Vulnerability in Windows Shell Could Allow Remote Code Execution (3041836)**

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

Risk Level: High

CVE: CVE-2015-0081, CVE-2015-0096

#### Update Details

Recommendation is updated

### **18011 - (MS15-018) Cumulative Security Update for Internet Explorer (3032359)**

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

Risk Level: High

CVE: CVE-2015-0032, CVE-2015-0056, CVE-2015-0072, CVE-2015-0099, CVE-2015-0100, CVE-2015-1622, CVE-2015-1623, CVE-2015-1624, CVE-2015-1625, CVE-2015-1626, CVE-2015-1627, CVE-2015-1634

[Update Details](#)

Recommendation is updated

#### **18013 - (MS15-018) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3032359)**

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

Risk Level: High

CVE: CVE-2015-0056

[Update Details](#)

Recommendation is updated

#### **18015 - (MS15-018) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3032359)**

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

Risk Level: High

CVE: CVE-2015-0099

[Update Details](#)

Recommendation is updated

#### **18016 - (MS15-018) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3032359)**

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

Risk Level: High

CVE: CVE-2015-0100

[Update Details](#)

Recommendation is updated

#### **18017 - (MS15-018) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3032359)**

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

Risk Level: High

CVE: CVE-2015-1622

[Update Details](#)

Recommendation is updated

#### **18018 - (MS15-018) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3032359)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1634

[Update Details](#)

Recommendation is updated

#### **18019 - (MS15-018) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (3032359)**

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

Risk Level: High

CVE: CVE-2015-1623

[Update Details](#)

Recommendation is updated

#### **18020 - (MS15-018) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3032359)**

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

Risk Level: High

CVE: CVE-2015-1624

[Update Details](#)

Recommendation is updated

#### **18021 - (MS15-018) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3032359)**

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

Risk Level: High

CVE: CVE-2015-1625

[Update Details](#)

Recommendation is updated

#### **18022 - (MS15-018) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3032359)**

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

Risk Level: High

CVE: CVE-2015-1626

[Update Details](#)

Recommendation is updated

#### **18023 - (MS15-018) Microsoft Internet Explorer VBScript Memory Corruption Remote Code Execution (3032359)**

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

Risk Level: High

CVE: CVE-2015-0032

[Update Details](#)

Recommendation is updated

**18138 - (MS15-032) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3038314)**

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

Risk Level: High

CVE: CVE-2015-1652

[Update Details](#)

Recommendation is updated

**18139 - (MS15-032) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3038314)**

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

Risk Level: High

CVE: CVE-2015-1657

[Update Details](#)

Recommendation is updated

**18140 - (MS15-032) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3038314)**

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

Risk Level: High

CVE: CVE-2015-1659

[Update Details](#)

Recommendation is updated

**18141 - (MS15-032) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3038314)**

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

Risk Level: High

CVE: CVE-2015-1660

[Update Details](#)

Recommendation is updated

**18143 - (MS15-032) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3038314)**

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

Risk Level: High

CVE: CVE-2015-1662



[Update Details](#)

Recommendation is updated

**18144 - (MS15-032) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3038314)**

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

Risk Level: High

CVE: CVE-2015-1665

[Update Details](#)

Recommendation is updated

**18145 - (MS15-032) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3038314)**

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

Risk Level: High

CVE: CVE-2015-1666

[Update Details](#)

Recommendation is updated

**18146 - (MS15-032) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3038314)**

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

Risk Level: High

CVE: CVE-2015-1667

[Update Details](#)

Recommendation is updated

**18147 - (MS15-032) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3038314)**

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

Risk Level: High

CVE: CVE-2015-1668

[Update Details](#)

Recommendation is updated

**18152 - (MS15-033) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3048019)**

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

Risk Level: High

CVE: CVE-2015-1639, CVE-2015-1641, CVE-2015-1642, CVE-2015-1649, CVE-2015-1650, CVE-2015-1651

[Update Details](#)

Recommendation is updated

#### **18154 - (MS15-033) Microsoft Office Component Use-After-Free Remote Code Execution IV (3048019)**

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

Risk Level: High

CVE: CVE-2015-1651

[Update Details](#)

Recommendation is updated

#### **18155 - (MS15-033) Microsoft Office Component Use-After-Free Remote Code Execution III (3048019)**

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

Risk Level: High

CVE: CVE-2015-1650

[Update Details](#)

Recommendation is updated

#### **18156 - (MS15-033) Microsoft Office Component Use-After-Free Remote Code Execution II (3048019)**

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

Risk Level: High

CVE: CVE-2015-1649

[Update Details](#)

Recommendation is updated

#### **18158 - (MS15-033) Microsoft Office Memory Corruption Remote Code Execution (3048019)**

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

Risk Level: High

CVE: CVE-2015-1641

[Update Details](#)

Recommendation is updated

#### **18159 - (MS15-032) Cumulative Security Update for Internet Explorer (3038314)**

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

Risk Level: High

CVE: CVE-2015-1652, CVE-2015-1657, CVE-2015-1659, CVE-2015-1660, CVE-2015-1661, CVE-2015-1662, CVE-2015-1665, CVE-2015-1666, CVE-2015-1667, CVE-2015-1668

[Update Details](#)

Recommendation is updated

### 18169 - (MS15-033) Microsoft Office Memory Corruption Remote Code Execution (3048019)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-1641

#### Update Details

Recommendation is updated

### 18263 - (MS15-046) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3057181)

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

Risk Level: High

CVE: CVE-2015-1682, CVE-2015-1683

#### Update Details

Recommendation is updated

### 18266 - (MS15-043) Cumulative Security Update for Internet Explorer (3049563)

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

Risk Level: High

CVE: CVE-2015-1658, CVE-2015-1684, CVE-2015-1685, CVE-2015-1686, CVE-2015-1688, CVE-2015-1689, CVE-2015-1691, CVE-2015-1692, CVE-2015-1694, CVE-2015-1703, CVE-2015-1704, CVE-2015-1705, CVE-2015-1706, CVE-2015-1708, CVE-2015-1709, CVE-2015-1710, CVE-2015-1711, CVE-2015-1712, CVE-2015-1713, CVE-2015-1714

#### Update Details

Recommendation is updated

### 18268 - (MS15-046) Microsoft Office Memory Corruption II Remote Code Execution (3057181)

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

Risk Level: High

CVE: CVE-2015-1683

#### Update Details

Recommendation is updated

### 18269 - (MS15-044) Vulnerabilities in GDI+ Could Allow Remote Code Execution (3057110)

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

Risk Level: High

CVE: CVE-2015-1670, CVE-2015-1671

#### Update Details

Recommendation is updated

### 18271 - (MS15-048) Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3057134)

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

Risk Level: High

CVE: CVE-2015-1672, CVE-2015-1673

#### Update Details

Recommendation is updated

### 18283 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3049563)

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

Risk Level: High

CVE: CVE-2015-1658

#### Update Details

Recommendation is updated

### 18288 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3049563)

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

Risk Level: High

CVE: CVE-2015-1689

#### Update Details

Recommendation is updated

### 18289 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3049563)

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

Risk Level: High

CVE: CVE-2015-1691

#### Update Details

Recommendation is updated

### 18292 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3049563)

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

Risk Level: High

CVE: CVE-2015-1694

#### Update Details

Recommendation is updated

### 18295 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3049563)

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

Risk Level: High

CVE: CVE-2015-1705

[Update Details](#)

Recommendation is updated

#### **18296 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution VI (3049563)**

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

Risk Level: High

CVE: CVE-2015-1706

[Update Details](#)

Recommendation is updated

#### **18297 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution VII (3049563)**

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

Risk Level: High

CVE: CVE-2015-1708

[Update Details](#)

Recommendation is updated

#### **18298 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution VIII (3049563)**

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

Risk Level: High

CVE: CVE-2015-1709

[Update Details](#)

Recommendation is updated

#### **18300 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution IX (3049563)**

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

Risk Level: High

CVE: CVE-2015-1710

[Update Details](#)

Recommendation is updated

#### **18301 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution X (3049563)**

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

Risk Level: High  
CVE: CVE-2015-1711

[Update Details](#)

Recommendation is updated

**18302 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution XI (3049563)**

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

Risk Level: High  
CVE: CVE-2015-1712

[Update Details](#)

Recommendation is updated

**18304 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution XII (3049563)**

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

Risk Level: High  
CVE: CVE-2015-1714

[Update Details](#)

Recommendation is updated

**18306 - (MS15-044) Microsoft Windows GDI+ TrueType Font Parsing Remote Code Execution (3057110)**

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

Risk Level: High  
CVE: CVE-2015-1671

[Update Details](#)

Recommendation is updated

**18335 - (MS15-044) Microsoft Windows GDI+ TrueType Font Parsing Remote Code Execution (3057110)**

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High  
CVE: CVE-2015-1671

[Update Details](#)

Recommendation is updated

**18339 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIII (3049563)**

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

Risk Level: High  
CVE: CVE-2015-1717

[Update Details](#)

Recommendation is updated

**18340 - (MS15-043) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIV (3049563)**

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

Risk Level: High

CVE: CVE-2015-1718

[Update Details](#)

Recommendation is updated

**18425 - (MS15-056) Cumulative Security Update for Internet Explorer (3058515)**

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

Risk Level: High

CVE: CVE-2015-1687, CVE-2015-1730, CVE-2015-1731, CVE-2015-1732, CVE-2015-1735, CVE-2015-1736, CVE-2015-1737, CVE-2015-1739, CVE-2015-1740, CVE-2015-1741, CVE-2015-1742, CVE-2015-1743, CVE-2015-1744, CVE-2015-1745, CVE-2015-1747, CVE-2015-1748, CVE-2015-1750, CVE-2015-1751, CVE-2015-1752, CVE-2015-1753, CVE-2015-1754, CVE-2015-1755, CVE-2015-1765, CVE-2015-1766

[Update Details](#)

Recommendation is updated

**18427 - (MS15-056) Microsoft Internet Explorer Memory Corruption XXII Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1766

[Update Details](#)

Recommendation is updated

**18429 - (MS15-056) Microsoft Internet Explorer Memory Corruption XXI Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1755

[Update Details](#)

Recommendation is updated

**18430 - (MS15-056) Microsoft Internet Explorer Memory Corruption XX Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1754

[Update Details](#)

Recommendation is updated

**18431 - (MS15-056) Microsoft Internet Explorer Memory Corruption XIX Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1753

[Update Details](#)

Recommendation is updated

**18432 - (MS15-056) Microsoft Internet Explorer Memory Corruption XVIII Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1752

[Update Details](#)

Recommendation is updated

**18433 - (MS15-056) Microsoft Internet Explorer Memory Corruption XVII Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1751

[Update Details](#)

Recommendation is updated

**18434 - (MS15-056) Microsoft Internet Explorer Memory Corruption XVI Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1750

[Update Details](#)

Recommendation is updated

**18436 - (MS15-056) Microsoft Internet Explorer Memory Corruption XV Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1747

[Update Details](#)



Recommendation is updated

#### **18437 - (MS15-056) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1745

[Update Details](#)

Recommendation is updated

#### **18438 - (MS15-056) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1744

[Update Details](#)

Recommendation is updated

#### **18440 - (MS15-056) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1742

[Update Details](#)

Recommendation is updated

#### **18441 - (MS15-056) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1741

[Update Details](#)

Recommendation is updated

#### **18442 - (MS15-056) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1740

[Update Details](#)

Recommendation is updated

---

#### 18445 - (MS15-056) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1737

##### Update Details

Recommendation is updated

#### 18446 - (MS15-056) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1736

##### Update Details

Recommendation is updated

#### 18447 - (MS15-056) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1735

##### Update Details

Recommendation is updated

#### 18449 - (MS15-056) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1732

##### Update Details

Recommendation is updated

#### 18450 - (MS15-056) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1731

##### Update Details

Recommendation is updated

#### 18451 - (MS15-056) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3058515)

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

Risk Level: High

CVE: CVE-2015-1730

Update Details

Recommendation is updated

**18452 - (MS15-056) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3058515)**

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

Risk Level: High

CVE: CVE-2015-1687

Update Details

Recommendation is updated

**18457 - (MS15-057) Microsoft Windows Media Player DataObject Remote Code Execution (3033890)**

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

Risk Level: High

CVE: CVE-2015-1728

Update Details

Recommendation is updated

**18466 - (MS15-057) Vulnerability in Windows Media Player Could Allow Remote Code Execution (3033890)**

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

Risk Level: High

CVE: CVE-2015-1728

Update Details

Recommendation is updated

**18591 - (MS15-065) Security Update for Internet Explorer (3076321)**

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

Risk Level: High

CVE: CVE-2015-1729, CVE-2015-1733, CVE-2015-1738, CVE-2015-1767, CVE-2015-2372, CVE-2015-2383, CVE-2015-2384, CVE-2015-2385, CVE-2015-2388, CVE-2015-2389, CVE-2015-2390, CVE-2015-2391, CVE-2015-2397, CVE-2015-2398, CVE-2015-2401, CVE-2015-2402, CVE-2015-2403, CVE-2015-2404, CVE-2015-2406, CVE-2015-2408, CVE-2015-2410, CVE-2015-2411, CVE-2015-2412, CVE-2015-2413, CVE-2015-2414, CVE-2015-2419, CVE-2015-2421, CVE-2015-2422, CVE-2015-2425

Update Details

Recommendation is updated

**18608 - (MS15-070) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3072620)**

---

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

Risk Level: High

CVE: CVE-2015-2375, CVE-2015-2376, CVE-2015-2377, CVE-2015-2378, CVE-2015-2379, CVE-2015-2380, CVE-2015-2415, CVE-2015-2424

[Update Details](#)

Recommendation is updated

#### **18611 - (MS15-070) Microsoft Office Memory Corruption Remote Code Execution V (3072620)**

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

Risk Level: High

CVE: CVE-2015-2415

[Update Details](#)

Recommendation is updated

#### **18612 - (MS15-070) Microsoft Office Memory Corruption Remote Code Execution IV (3072620)**

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

Risk Level: High

CVE: CVE-2015-2380

[Update Details](#)

Recommendation is updated

#### **18613 - (MS15-070) Microsoft Office Memory Corruption Remote Code Execution III (3072620)**

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

Risk Level: High

CVE: CVE-2015-2379

[Update Details](#)

Recommendation is updated

#### **18614 - (MS15-070) Microsoft Office Memory Corruption Remote Code Execution II (3072620)**

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

Risk Level: High

CVE: CVE-2015-2377

[Update Details](#)

Recommendation is updated

#### **18615 - (MS15-070) Microsoft Office Memory Corruption Remote Code Execution I (3072620)**

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

Risk Level: High

CVE: CVE-2015-2376

Update Details

Recommendation is updated

**18620 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3076321)**

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

Risk Level: High

CVE: CVE-2015-1733

Update Details

Recommendation is updated

**18621 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3076321)**

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

Risk Level: High

CVE: CVE-2015-1738

Update Details

Recommendation is updated

**18623 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3076321)**

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

Risk Level: High

CVE: CVE-2015-1767

Update Details

Recommendation is updated

**18624 - (MS15-065) Microsoft Internet Explorer VBScript Memory Corruption Remote Code Execution (3076321)**

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

Risk Level: High

CVE: CVE-2015-2372

Update Details

Recommendation is updated

**18626 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3076321)**

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

Risk Level: High

CVE: CVE-2015-2383

[Update Details](#)

Recommendation is updated

**18627 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3076321)**

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

Risk Level: High

CVE: CVE-2015-2384

[Update Details](#)

Recommendation is updated

**18628 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution VI (3076321)**

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

Risk Level: High

CVE: CVE-2015-2385

[Update Details](#)

Recommendation is updated

**18629 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution VII (3076321)**

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

Risk Level: High

CVE: CVE-2015-2388

[Update Details](#)

Recommendation is updated

**18630 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution VIII (3076321)**

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

Risk Level: High

CVE: CVE-2015-2389

[Update Details](#)

Recommendation is updated

**18631 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution IX (3076321)**

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

Risk Level: High

CVE: CVE-2015-2390

[Update Details](#)

Recommendation is updated

**18632 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution X (3076321)**

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

Risk Level: High

CVE: CVE-2015-2391

[Update Details](#)

Recommendation is updated

**18633 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XI (3076321)**

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

Risk Level: High

CVE: CVE-2015-2397

[Update Details](#)

Recommendation is updated

**18635 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XII (3076321)**

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

Risk Level: High

CVE: CVE-2015-2401

[Update Details](#)

Recommendation is updated

**18636 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIII (3076321)**

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

Risk Level: High

CVE: CVE-2015-2403

[Update Details](#)

Recommendation is updated

**18637 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIV (3076321)**

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

Risk Level: High

CVE: CVE-2015-2404

[Update Details](#)

Recommendation is updated

#### **18638 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XV (3076321)**

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

Risk Level: High

CVE: CVE-2015-2406

[Update Details](#)

Recommendation is updated

#### **18640 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVI (3076321)**

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

Risk Level: High

CVE: CVE-2015-2408

[Update Details](#)

Recommendation is updated

#### **18643 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVII (3076321)**

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

Risk Level: High

CVE: CVE-2015-2411

[Update Details](#)

Recommendation is updated

#### **18647 - (MS15-065) Microsoft Internet Explorer JScript9 Memory Corruption Remote Code Execution (3076321)**

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

Risk Level: High

CVE: CVE-2015-2419

[Update Details](#)

Recommendation is updated

#### **18649 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVIII (3076321)**

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

Risk Level: High

CVE: CVE-2015-2422

[Update Details](#)

Recommendation is updated



### 18657 - (MS15-070) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3072620)

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-2375, CVE-2015-2376, CVE-2015-2377, CVE-2015-2378, CVE-2015-2379, CVE-2015-2380, CVE-2015-2415, CVE-2015-2424

#### [Update Details](#)

Recommendation is updated

### 18658 - (MS15-065) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIX (3076321)

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

Risk Level: High

CVE: CVE-2015-2425

#### [Update Details](#)

Recommendation is updated

### 18762 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3082442)

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

Risk Level: High

CVE: CVE-2015-2441

#### [Update Details](#)

Recommendation is updated

### 18763 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3082442)

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

Risk Level: High

CVE: CVE-2015-2442

#### [Update Details](#)

Recommendation is updated

### 18764 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3082442)

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

Risk Level: High

CVE: CVE-2015-2443

#### [Update Details](#)

Recommendation is updated

### 18765 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3082442)

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

Risk Level: High

CVE: CVE-2015-2444

Update Details

Recommendation is updated

**18766 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3082442)**

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

Risk Level: High

CVE: CVE-2015-2446

Update Details

Recommendation is updated

**18767 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution VI (3082442)**

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

Risk Level: High

CVE: CVE-2015-2447

Update Details

Recommendation is updated

**18768 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution VII (3082442)**

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

Risk Level: High

CVE: CVE-2015-2448

Update Details

Recommendation is updated

**18769 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution VIII (3082442)**

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

Risk Level: High

CVE: CVE-2015-2450

Update Details

Recommendation is updated

**18770 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution IX (3082442)**

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

Risk Level: High  
CVE: CVE-2015-2451

[Update Details](#)

Recommendation is updated

**18771 - (MS15-079) Microsoft Internet Explorer Memory Corruption Remote Code Execution X (3082442)**

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

Risk Level: High  
CVE: CVE-2015-2452

[Update Details](#)

Recommendation is updated

**18781 - (MS15-079) Cumulative Security Update for Internet Explorer (3082442)**

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

Risk Level: High  
CVE: CVE-2015-2423, CVE-2015-2441, CVE-2015-2442, CVE-2015-2443, CVE-2015-2444, CVE-2015-2445, CVE-2015-2446, CVE-2015-2447, CVE-2015-2448, CVE-2015-2449, CVE-2015-2450, CVE-2015-2451, CVE-2015-2452

[Update Details](#)

Recommendation is updated

**18782 - (MS15-080) Microsoft Office Graphics Component Remote Code Execution (3078662)**

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

Risk Level: High  
CVE: CVE-2015-2431

[Update Details](#)

Recommendation is updated

**18783 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution I (3078662)**

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

Risk Level: High  
CVE: CVE-2015-2432

[Update Details](#)

Recommendation is updated

**18784 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution I (3078662)**

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

Risk Level: High

CVE: CVE-2015-2435

[Update Details](#)

Recommendation is updated

**18785 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution II (3078662)**

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

Risk Level: High

CVE: CVE-2015-2455

[Update Details](#)

Recommendation is updated

**18786 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution III (3078662)**

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

Risk Level: High

CVE: CVE-2015-2456

[Update Details](#)

Recommendation is updated

**18787 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution II (3078662)**

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

Risk Level: High

CVE: CVE-2015-2458

[Update Details](#)

Recommendation is updated

**18788 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution III (3078662)**

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

Risk Level: High

CVE: CVE-2015-2459

[Update Details](#)

Recommendation is updated

**18789 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution IV (3078662)**

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

Risk Level: High

CVE: CVE-2015-2460

[Update Details](#)

Recommendation is updated

**18790 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution V (3078662)**

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

Risk Level: High

CVE: CVE-2015-2461

[Update Details](#)

Recommendation is updated

**18791 - (MS15-080) Microsoft Windows OpenType Font Parsing Remote Code Execution VI (3078662)**

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

Risk Level: High

CVE: CVE-2015-2462

[Update Details](#)

Recommendation is updated

**18792 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution IV (3078662)**

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

Risk Level: High

CVE: CVE-2015-2463

[Update Details](#)

Recommendation is updated

**18793 - (MS15-080) Microsoft Windows TrueType Font Parsing Remote Code Execution V (3078662)**

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

Risk Level: High

CVE: CVE-2015-2464

[Update Details](#)

Recommendation is updated

**18797 - (MS15-081) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3080790)**

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

Risk Level: High

CVE: CVE-2015-1642, CVE-2015-2423, CVE-2015-2466, CVE-2015-2467, CVE-2015-2468, CVE-2015-2469, CVE-2015-2470, CVE-2015-2477

[Update Details](#)

Recommendation is updated

### **18801 - (MS15-091) Microsoft Edge Memory Corruption I Remote Code Execution (3084525)**

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

Risk Level: High

CVE: CVE-2015-2441

[Update Details](#)

Recommendation is updated

### **18802 - (MS15-091) Microsoft Edge Memory Corruption II Remote Code Execution (3084525)**

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

Risk Level: High

CVE: CVE-2015-2442

[Update Details](#)

Recommendation is updated

### **18803 - (MS15-091) Microsoft Edge Memory Corruption III Remote Code Execution (3084525)**

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

Risk Level: High

CVE: CVE-2015-2446

[Update Details](#)

Recommendation is updated

### **18805 - (MS15-080) Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)**

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

Risk Level: High

CVE: CVE-2015-2431, CVE-2015-2432, CVE-2015-2433, CVE-2015-2435, CVE-2015-2453, CVE-2015-2454, CVE-2015-2455, CVE-2015-2456, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461, CVE-2015-2462, CVE-2015-2463, CVE-2015-2464, CVE-2015-2465

[Update Details](#)

Recommendation is updated

### **18808 - (MS15-091) Cumulative Security Update for Microsoft Edge (3084525)**

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

Risk Level: High

CVE: CVE-2015-2441, CVE-2015-2442, CVE-2015-2446, CVE-2015-2449

[Update Details](#)

Recommendation is updated

### **18810 - (MS15-080) Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)**

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-2431, CVE-2015-2432, CVE-2015-2433, CVE-2015-2435, CVE-2015-2453, CVE-2015-2454, CVE-2015-2455, CVE-2015-2456, CVE-2015-2458, CVE-2015-2459, CVE-2015-2460, CVE-2015-2461, CVE-2015-2462, CVE-2015-2463, CVE-2015-2464, CVE-2015-2465

[Update Details](#)

Recommendation is updated

### **18820 - (MS15-092) Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3086251)**

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

Risk Level: High

CVE: CVE-2015-2479, CVE-2015-2480, CVE-2015-2481

[Update Details](#)

Recommendation is updated

### **18822 - (MS15-081) Microsoft Office Memory Corruption I Remote Code Execution (3080790)**

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

Risk Level: High

CVE: CVE-2015-1642

[Update Details](#)

Recommendation is updated

### **18824 - (MS15-081) Microsoft Office Memory Corruption II Remote Code Execution (3080790)**

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

Risk Level: High

CVE: CVE-2015-2466

[Update Details](#)

Recommendation is updated

### **18825 - (MS15-081) Microsoft Office Memory Corruption III Remote Code Execution (3080790)**

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

Risk Level: High

CVE: CVE-2015-2467

[Update Details](#)

Recommendation is updated

### 18826 - (MS15-081) Microsoft Office Memory Corruption IV Remote Code Execution (3080790)

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

Risk Level: High

CVE: CVE-2015-2468

#### Update Details

Recommendation is updated

### 18827 - (MS15-081) Microsoft Office Memory Corruption V Remote Code Execution (3080790)

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

Risk Level: High

CVE: CVE-2015-2469

#### Update Details

Recommendation is updated

### 18828 - (MS15-081) Microsoft Office Memory Corruption Integer Underflow Remote Code Execution (3080790)

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

Risk Level: High

CVE: CVE-2015-2470

#### Update Details

Recommendation is updated

### 18829 - (MS15-081) Microsoft Office Memory Corruption VI Remote Code Execution (3080790)

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

Risk Level: High

CVE: CVE-2015-2477

#### Update Details

Recommendation is updated

### 18835 - (MS15-092) Microsoft .NET Framework RyuJIT Optimization Privilege Escalation I (3086251)

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

Risk Level: High

CVE: CVE-2015-2479

#### Update Details

Recommendation is updated

### 18836 - (MS15-092) Microsoft .NET Framework RyuJIT Optimization Privilege Escalation II (3086251)



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

Risk Level: High

CVE: CVE-2015-2480

[Update Details](#)

Recommendation is updated

### 18837 - (MS15-092) Microsoft .NET Framework RyuJIT Optimization Privilege Escalation III (3086251)

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

Risk Level: High

CVE: CVE-2015-2481

[Update Details](#)

Recommendation is updated

### 18838 - (MS15-081) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3080790)

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-1642, CVE-2015-2423, CVE-2015-2466, CVE-2015-2467, CVE-2015-2468, CVE-2015-2469, CVE-2015-2470, CVE-2015-2477

[Update Details](#)

Recommendation is updated

### 18846 - (MS15-093) Microsoft Internet Explorer Memory Corruption Remote Code Execution (3088903)

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

Risk Level: High

CVE: CVE-2015-2502

[Update Details](#)

Recommendation is updated

### 18919 - (MS15-101) Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3089662)

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

Risk Level: High

CVE: CVE-2015-2504

[Update Details](#)

Recommendation is updated

### 18920 - (MS15-101) Microsoft .NET Framework Object Copy Privilege Escalation (3089662)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2504

[Update Details](#)

Recommendation is updated

### 18928 - (MS15-094) Cumulative Security Update for Internet Explorer (3089548)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2483, CVE-2015-2484, CVE-2015-2485, CVE-2015-2486, CVE-2015-2487, CVE-2015-2489, CVE-2015-2490, CVE-2015-2491, CVE-2015-2492, CVE-2015-2498, CVE-2015-2499, CVE-2015-2500, CVE-2015-2501, CVE-2015-2541, CVE-2015-2542

[Update Details](#)

Recommendation is updated

### 18929 - (MS15-094) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (3089548)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2486

[Update Details](#)

Recommendation is updated

### 18930 - (MS15-094) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (3089548)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2485

[Update Details](#)

Recommendation is updated

### 18933 - (MS15-094) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (3089548)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2490

[Update Details](#)

Recommendation is updated

### 18935 - (MS15-094) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3089548)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2015-2487

[Update Details](#)

Recommendation is updated

**18936 - (MS15-094) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (3089548)**

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

Risk Level: High  
CVE: CVE-2015-2499

[Update Details](#)

Recommendation is updated

**18937 - (MS15-094) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (3089548)**

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

Risk Level: High  
CVE: CVE-2015-2498

[Update Details](#)

Recommendation is updated

**18938 - (MS15-094) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (3089548)**

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

Risk Level: High  
CVE: CVE-2015-2492

[Update Details](#)

Recommendation is updated

**18939 - (MS15-094) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (3089548)**

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

Risk Level: High  
CVE: CVE-2015-2491

[Update Details](#)

Recommendation is updated

**18940 - (MS15-094) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3089548)**

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

Risk Level: High  
CVE: CVE-2015-2542

[Update Details](#)

Recommendation is updated

**18941 - (MS15-094) Microsoft Internet Explorer Memory Corruption XIII Remote Code Execution (3089548)**

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

Risk Level: High

CVE: CVE-2015-2541

[Update Details](#)

Recommendation is updated

**18942 - (MS15-094) Microsoft Internet Explorer Memory Corruption XII Remote Code Execution (3089548)**

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

Risk Level: High

CVE: CVE-2015-2501

[Update Details](#)

Recommendation is updated

**18943 - (MS15-094) Microsoft Internet Explorer Memory Corruption XI Remote Code Execution (3089548)**

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

Risk Level: High

CVE: CVE-2015-2500

[Update Details](#)

Recommendation is updated

**18944 - (MS15-099) Microsoft Office Memory Corruption III Remote Code Execution (3089664)**

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

Risk Level: High

CVE: CVE-2015-2523

[Update Details](#)

Recommendation is updated

**18946 - (MS15-099) Microsoft Office Memory Corruption II Remote Code Execution (3089664)**

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

Risk Level: High

CVE: CVE-2015-2521

[Update Details](#)

Recommendation is updated

#### **18947 - (MS15-099) Microsoft Office Memory Corruption I Remote Code Execution (3089664)**

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

Risk Level: High

CVE: CVE-2015-2520

#### Update Details

Recommendation is updated

#### **18948 - (MS15-099) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3089664)**

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

Risk Level: High

CVE: CVE-2015-2520, CVE-2015-2521, CVE-2015-2522, CVE-2015-2523

#### Update Details

Recommendation is updated

#### **18949 - (MS15-099) Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3089664)**

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-2520, CVE-2015-2521, CVE-2015-2522, CVE-2015-2523

#### Update Details

Recommendation is updated

#### **18960 - (MS15-097) Microsoft Windows Graphics OpenType Font Parsing Denial of Service (3089656)**

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

Risk Level: High

CVE: CVE-2015-2506, CVE-2016-3679

#### Update Details

Recommendation is updated

#### **18963 - (MS15-097) Microsoft Windows Graphics Font Parsing Remote Code Execution (3089656)**

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

Risk Level: High

CVE: CVE-2015-2510

#### Update Details

Recommendation is updated

### 18969 - (MS15-094) Microsoft Internet Explorer Memory Corruption XIV Remote Code Execution (3089548)

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

Risk Level: High

CVE: CVE-2015-2494

#### Update Details

Recommendation is updated

### 18970 - (MS15-094) Microsoft Internet Explorer Scripting Engine Remote Code Execution(3089548)

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

Risk Level: High

CVE: CVE-2015-2493

#### Update Details

Recommendation is updated

### 18973 - (MS15-098) Microsoft Windows Journal I Remote Code Execution (3089669)

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

Risk Level: High

CVE: CVE-2015-2513

#### Update Details

Recommendation is updated

### 18974 - (MS15-098) Microsoft Windows Journal II Remote Code Execution (3089669)

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

Risk Level: High

CVE: CVE-2015-2514

#### Update Details

Recommendation is updated

### 18976 - (MS15-098) Microsoft Windows Journal Remote Code Execution (3089669)

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

Risk Level: High

CVE: CVE-2015-2519

#### Update Details

Recommendation is updated

### 18977 - (MS15-098) Microsoft Windows Journal III Remote Code Execution (3089669)

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

Risk Level: High

CVE: CVE-2015-2530

Update Details

Recommendation is updated

**18978 - (MS15-095) Microsoft Edge Memory Corruption I Remote Code Execution (3089665)**

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

Risk Level: High

CVE: CVE-2015-2485

Update Details

Recommendation is updated

**18979 - (MS15-095) Microsoft Edge Memory Corruption II Remote Code Execution (3089665)**

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

Risk Level: High

CVE: CVE-2015-2486

Update Details

Recommendation is updated

**18980 - (MS15-095) Microsoft Edge Memory Corruption III Remote Code Execution (3089665)**

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

Risk Level: High

CVE: CVE-2015-2494

Update Details

Recommendation is updated

**18981 - (MS15-095) Microsoft Edge Memory Corruption IV Remote Code Execution (3089665)**

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

Risk Level: High

CVE: CVE-2015-2542

Update Details

Recommendation is updated

**18983 - (MS15-095) Cumulative Security Update for Microsoft Edge (3089665)**

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

Risk Level: High

CVE: CVE-2015-2485, CVE-2015-2486, CVE-2015-2494, CVE-2015-2542

Update Details

Recommendation is updated

**18984 - (MS15-097) Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3089656)**

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

Risk Level: High

CVE: CVE-2015-2506, CVE-2015-2507, CVE-2015-2508, CVE-2015-2510, CVE-2015-2511, CVE-2015-2512, CVE-2015-2517, CVE-2015-2518, CVE-2015-2527, CVE-2015-2529, CVE-2015-2546

Update Details

Recommendation is updated

**18985 - (MS15-098) Vulnerabilities in Windows Journal Could Allow Remote Code Execution (3089669)**

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

Risk Level: High

CVE: CVE-2015-2513, CVE-2015-2514, CVE-2015-2516, CVE-2015-2519, CVE-2015-2530

Update Details

Recommendation is updated

**18989 - (MS15-099) Microsoft Office Malformed EPS File Remote Code Execution (3089664)**

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

Risk Level: High

CVE: CVE-2015-2545

Update Details

Recommendation is updated

**19077 - (MS15-109) Security Update for Windows Shell to Address Remote Code Execution (3096443)**

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

Risk Level: High

CVE: CVE-2015-2515, CVE-2015-2548

Update Details

Recommendation is updated

**19078 - (MS15-109) Microsoft Windows Toolbar Use-After Free Remote Code Execution (3096443)**

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

Risk Level: High



CVE: CVE-2015-2515

Update Details

Recommendation is updated

**19079 - (MS15-109) Microsoft Windows Tablet Input Band Use-After Free Remote Code Execution (3096443)**

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

Risk Level: High

CVE: CVE-2015-2548

Update Details

Recommendation is updated

**19080 - (MS15-106) Microsoft Internet Explorer Scripting Engine Memory Corruption I Remote Code Execution (3096441)**

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

Risk Level: High

CVE: CVE-2015-2482

Update Details

Recommendation is updated

**19081 - (MS15-106) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (3096441)**

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

Risk Level: High

CVE: CVE-2015-6042

Update Details

Recommendation is updated

**19082 - (MS15-110) Microsoft Office Memory Corruption Remote Code Execution I (3089664)**

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

Risk Level: High

CVE: CVE-2015-2555

Update Details

Recommendation is updated

**19089 - (MS15-106) Microsoft Internet Explorer Memory Corruption Remote Code Execution (3096441)**

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

Risk Level: High

CVE: CVE-2015-6048

[Update Details](#)

Recommendation is updated

**19090 - (MS15-106) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (3096441)**

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

Risk Level: High

CVE: CVE-2015-6049

[Update Details](#)

Recommendation is updated

**19091 - (MS15-106) Microsoft Internet Explorer Remote Code Execution (3096441)**

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

Risk Level: High

CVE: CVE-2015-6050

[Update Details](#)

Recommendation is updated

**19095 - (MS15-106) Microsoft Internet Explorer Scripting Engine Memory Corruption II Remote Code Execution (3096441)**

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

Risk Level: High

CVE: CVE-2015-6055

[Update Details](#)

Recommendation is updated

**19096 - (MS15-106) Microsoft Internet Explorer Scripting Engine Memory Corruption III Remote Code Execution (3096441)**

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

Risk Level: High

CVE: CVE-2015-6056

[Update Details](#)

Recommendation is updated

**19103 - (MS15-106) Cumulative Security Update for Internet Explorer (3096441)**

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

Risk Level: High

CVE: CVE-2015-2482, CVE-2015-6042, CVE-2015-6043, CVE-2015-6044, CVE-2015-6045, CVE-2015-6046, CVE-2015-6047, CVE-2015-6048, CVE-2015-6049, CVE-2015-6050, CVE-2015-6051, CVE-2015-6052, CVE-2015-6053, CVE-2015-6055, CVE-2015-6056, CVE-2015-6059

[Update Details](#)

Recommendation is updated

**19105 - (MS15-110) Microsoft Office Memory Corruption Remote Code Execution II (3089664)**

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

Risk Level: High

CVE: CVE-2015-2557

[Update Details](#)

Recommendation is updated

**19106 - (MS15-110) Microsoft Office Memory Corruption Remote Code Execution III (3089664)**

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

Risk Level: High

CVE: CVE-2015-2558

[Update Details](#)

Recommendation is updated

**19109 - (MS15-110) Security Updates for Microsoft Office to Address Remote Code Execution**

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

Risk Level: High

CVE: CVE-2015-2555, CVE-2015-2556, CVE-2015-2557, CVE-2015-2558, CVE-2015-6037, CVE-2015-6039

[Update Details](#)

Recommendation is updated

**19120 - (MS15-110) Security Updates for Microsoft Office to Address Remote Code Execution**

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-2555, CVE-2015-2556, CVE-2015-2557, CVE-2015-2558, CVE-2015-6037, CVE-2015-6039

[Update Details](#)

Recommendation is updated

**19206 - (MS15-116) Microsoft Office COM Control Privilege Escalation (3104540)**

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

Risk Level: High

CVE: CVE-2015-2503

[Update Details](#)

Recommendation is updated

### 19207 - (MS15-116) Microsoft Office Memory Corruption Remote Code Execution V (3104540)

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

Risk Level: High

CVE: CVE-2015-6038

#### Update Details

Recommendation is updated

### 19208 - (MS15-116) Microsoft Office Memory Corruption Remote Code Execution I (3104540)

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

Risk Level: High

CVE: CVE-2015-6091

#### Update Details

Recommendation is updated

### 19209 - (MS15-116) Microsoft Office Memory Corruption Remote Code Execution II (3104540)

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

Risk Level: High

CVE: CVE-2015-6092

#### Update Details

Recommendation is updated

### 19210 - (MS15-116) Microsoft Office Memory Corruption Remote Code Execution III (3104540)

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

Risk Level: High

CVE: CVE-2015-6093

#### Update Details

Recommendation is updated

### 19211 - (MS15-116) Microsoft Office Memory Corruption Remote Code Execution IV (3104540)

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

Risk Level: High

CVE: CVE-2015-6094

#### Update Details

Recommendation is updated

### 19212 - (MS15-116) Security Updates for Microsoft Office to Address Remote Code Execution (3104540)

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

Risk Level: High

CVE: CVE-2015-2503, CVE-2015-6038, CVE-2015-6091, CVE-2015-6092, CVE-2015-6093, CVE-2015-6094, CVE-2015-6123

Update Details

Recommendation is updated

**19213 - (MS15-116) Security Updates for Microsoft Office to Address Remote Code Execution (3104540)**

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-2503, CVE-2015-6038, CVE-2015-6091, CVE-2015-6092, CVE-2015-6093, CVE-2015-6094, CVE-2015-6123

Update Details

Recommendation is updated

**19218 - (MS15-113) Cumulative Security Update for Microsoft Edge (3104519)**

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

Risk Level: High

CVE: CVE-2015-6064, CVE-2015-6073, CVE-2015-6078, CVE-2015-6088

Update Details

Recommendation is updated

**19219 - (MS15-113) Microsoft Edge Memory Corruption Remote Code Execution III (3104519)**

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

Risk Level: High

CVE: CVE-2015-6078

Update Details

Recommendation is updated

**19220 - (MS15-113) Microsoft Edge Memory Corruption Remote Code Execution II (3104519)**

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

Risk Level: High

CVE: CVE-2015-6073

Update Details

Recommendation is updated

**19222 - (MS15-113) Microsoft Edge Memory Corruption Remote Code Execution I (3104519)**

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

Risk Level: High

CVE: CVE-2015-6064

Update Details

Recommendation is updated

**19223 - (MS15-115) Security Update for Microsoft Windows to Address Remote Code Execution (3105864)**

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

Risk Level: High

CVE: CVE-2015-6100, CVE-2015-6101, CVE-2015-6102, CVE-2015-6103, CVE-2015-6104, CVE-2015-6109, CVE-2015-6113

Update Details

Recommendation is updated

**19227 - (MS15-115) Microsoft Windows Adobe Type Manager Library OpenType Fonts Remote Code Execution I (3105864)**

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

Risk Level: High

CVE: CVE-2015-6103

Update Details

Recommendation is updated

**19228 - (MS15-115) Microsoft Windows Adobe Type Manager Library OpenType Fonts Remote Code Execution II (3105864)**

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

Risk Level: High

CVE: CVE-2015-6104

Update Details

Recommendation is updated

**19242 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3104517)**

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

Risk Level: High

CVE: CVE-2015-2427

Update Details

Recommendation is updated

**19243 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3104517)**

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

Risk Level: High

CVE: CVE-2015-6064

[Update Details](#)

Recommendation is updated

**19244 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3104517)**

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

Risk Level: High

CVE: CVE-2015-6065

[Update Details](#)

Recommendation is updated

**19245 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3104517)**

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

Risk Level: High

CVE: CVE-2015-6066

[Update Details](#)

Recommendation is updated

**19246 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3104517)**

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

Risk Level: High

CVE: CVE-2015-6068

[Update Details](#)

Recommendation is updated

**19247 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution VI (3104517)**

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

Risk Level: High

CVE: CVE-2015-6069

[Update Details](#)

Recommendation is updated

**19248 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution VII (3104517)**

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

Risk Level: High

CVE: CVE-2015-6070

[Update Details](#)

Recommendation is updated

#### **19249 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution VIII (3104517)**

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

Risk Level: High

CVE: CVE-2015-6071

[Update Details](#)

Recommendation is updated

#### **19250 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution X (3104517)**

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

Risk Level: High

CVE: CVE-2015-6073

[Update Details](#)

Recommendation is updated

#### **19251 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XI (3104517)**

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

Risk Level: High

CVE: CVE-2015-6074

[Update Details](#)

Recommendation is updated

#### **19252 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XII (3104517)**

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

Risk Level: High

CVE: CVE-2015-6075

[Update Details](#)

Recommendation is updated

#### **19253 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIII (3104517)**

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

Risk Level: High

CVE: CVE-2015-6076

[Update Details](#)

Recommendation is updated

---



#### 19254 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIV (3104517)

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

Risk Level: High

CVE: CVE-2015-6077

##### Update Details

Recommendation is updated

#### 19255 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XV (3104517)

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

Risk Level: High

CVE: CVE-2015-6078

##### Update Details

Recommendation is updated

#### 19256 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVI (3104517)

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

Risk Level: High

CVE: CVE-2015-6079

##### Update Details

Recommendation is updated

#### 19257 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVII (3104517)

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

Risk Level: High

CVE: CVE-2015-6080

##### Update Details

Recommendation is updated

#### 19258 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVIII (3104517)

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

Risk Level: High

CVE: CVE-2015-6081

##### Update Details

Recommendation is updated

#### 19259 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIX (3104517)

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

Risk Level: High

CVE: CVE-2015-6082

Update Details

Recommendation is updated

**19260 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XX (3104517)**

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

Risk Level: High

CVE: CVE-2015-6084

Update Details

Recommendation is updated

**19261 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XXI (3104517)**

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

Risk Level: High

CVE: CVE-2015-6085

Update Details

Recommendation is updated

**19263 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution XXII (3104517)**

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

Risk Level: High

CVE: CVE-2015-6087

Update Details

Recommendation is updated

**19265 - (MS15-112) Microsoft Internet Explorer Scripting Engine Remote Code Execution (3104517)**

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

Risk Level: High

CVE: CVE-2015-6089

Update Details

Recommendation is updated

**19266 - (MS15-112) Microsoft Internet Explorer Memory Corruption Remote Code Execution IX (3104517)**

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

Risk Level: High

CVE: CVE-2015-6072

Update Details

Recommendation is updated

**19267 - (MS15-112) Cumulative Security Update for Internet Explorer (3104517)**

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

Risk Level: High

CVE: CVE-2015-2427, CVE-2015-6064, CVE-2015-6065, CVE-2015-6066, CVE-2015-6068, CVE-2015-6069, CVE-2015-6070, CVE-2015-6071, CVE-2015-6072, CVE-2015-6073, CVE-2015-6074, CVE-2015-6075, CVE-2015-6076, CVE-2015-6077, CVE-2015-6078, CVE-2015-6079, CVE-2015-6080, CVE-2015-6081, CVE-2015-6082, CVE-2015-6084, CVE-2015-6085, CVE-2015-6086, CVE-2015-6087, CVE-2015-6088, CVE-2015-6089

Update Details

Recommendation is updated

**19334 - (MS15-128) Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)**

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

Risk Level: High

CVE: CVE-2015-6106, CVE-2015-6107, CVE-2015-6108

Update Details

Recommendation is updated

**19336 - (MS15-128) Microsoft Windows Graphics Memory Corruption Remote Code Execution II (3104503)**

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

Risk Level: High

CVE: CVE-2015-6107

Update Details

Recommendation is updated

**19337 - (MS15-128) Microsoft Windows Graphics Memory Corruption Remote Code Execution III (3104503)**

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

Risk Level: High

CVE: CVE-2015-6108

Update Details

Recommendation is updated

**19338 - (MS15-128) Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)**

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-6106, CVE-2015-6107, CVE-2015-6108

Update Details

Recommendation is updated

**19341 - (MS15-131) Security Update for Microsoft Office to Address Remote Code Execution (3116111)**

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

Risk Level: High

CVE: CVE-2015-6040, CVE-2015-6118, CVE-2015-6122, CVE-2015-6124, CVE-2015-6172, CVE-2015-6177

Update Details

Recommendation is updated

**19342 - (MS15-131) Microsoft Office Memory Corruption Remote Code Execution VI (3116111)**

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

Risk Level: High

CVE: CVE-2015-6177

Update Details

Recommendation is updated

**19343 - (MS15-131) Microsoft Office Memory Corruption Remote Code Execution V (3116111)**

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

Risk Level: High

CVE: CVE-2015-6172

Update Details

Recommendation is updated

**19344 - (MS15-131) Microsoft Office Memory Corruption Remote Code Execution IV (3116111)**

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

Risk Level: High

CVE: CVE-2015-6124

Update Details

Recommendation is updated

**19345 - (MS15-131) Microsoft Office Memory Corruption Remote Code Execution III (3116111)**

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

Risk Level: High

CVE: CVE-2015-6122

[Update Details](#)

Recommendation is updated

**19346 - (MS15-131) Microsoft Office Memory Corruption Remote Code Execution II (3116111)**

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

Risk Level: High

CVE: CVE-2015-6118

[Update Details](#)

Recommendation is updated

**19347 - (MS15-131) Microsoft Office Memory Corruption Remote Code Execution I (3116111)**

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

Risk Level: High

CVE: CVE-2015-6040

[Update Details](#)

Recommendation is updated

**19353 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3116180)**

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

Risk Level: High

CVE: CVE-2015-6083

[Update Details](#)

Recommendation is updated

**19354 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3116180)**

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

Risk Level: High

CVE: CVE-2015-6134

[Update Details](#)

Recommendation is updated

**19356 - (MS15-124) Microsoft Internet Explorer Script Engine Memory Corruption Remote Code Execution (3116180)**

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

Risk Level: High

CVE: CVE-2015-6136

[Update Details](#)

Recommendation is updated

#### **19359 - (MS15-124) Microsoft Internet Explorer Browser Content Privilege Escalation (3116180)**

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

Risk Level: High

CVE: CVE-2015-6139

[Update Details](#)

Recommendation is updated

#### **19360 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3116180)**

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

Risk Level: High

CVE: CVE-2015-6140

[Update Details](#)

Recommendation is updated

#### **19361 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3116180)**

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

Risk Level: High

CVE: CVE-2015-6141

[Update Details](#)

Recommendation is updated

#### **19362 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3116180)**

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

Risk Level: High

CVE: CVE-2015-6142

[Update Details](#)

Recommendation is updated

#### **19363 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution VI (3116180)**

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

Risk Level: High

CVE: CVE-2015-6143

[Update Details](#)

Recommendation is updated

### 19365 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution VII (3116180)

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

Risk Level: High

CVE: CVE-2015-6145

#### Update Details

Recommendation is updated

### 19366 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution VIII (3116180)

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

Risk Level: High

CVE: CVE-2015-6146

#### Update Details

Recommendation is updated

### 19367 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution IX (3116180)

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

Risk Level: High

CVE: CVE-2015-6147

#### Update Details

Recommendation is updated

### 19368 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution X (3116180)

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

Risk Level: High

CVE: CVE-2015-6148

#### Update Details

Recommendation is updated

### 19369 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XI (3116180)

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

Risk Level: High

CVE: CVE-2015-6149

#### Update Details

Recommendation is updated

### 19370 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XII (3116180)

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

Risk Level: High

CVE: CVE-2015-6150

Update Details

Recommendation is updated

**19371 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIII (3116180)**

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

Risk Level: High

CVE: CVE-2015-6151

Update Details

Recommendation is updated

**19372 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIV (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6152

Update Details

Recommendation is updated

**19373 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XV (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6153

Update Details

Recommendation is updated

**19374 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVI (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6154

Update Details

Recommendation is updated

**19375 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVII (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)



Risk Level: High

CVE: CVE-2015-6155

[Update Details](#)

Recommendation is updated

**19376 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XVIII (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6156

[Update Details](#)

Recommendation is updated

**19378 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIX (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6158

[Update Details](#)

Recommendation is updated

**19379 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XX (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6159

[Update Details](#)

Recommendation is updated

**19380 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XXI (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6160

[Update Details](#)

Recommendation is updated

**19382 - (MS15-124) Microsoft Internet Explorer Memory Corruption Remote Code Execution XXII (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6162

[Update Details](#)

Recommendation is updated

**19386 - (MS15-126) Microsoft JScript and VBScript Engine Memory Corruption Remote Code Execution I (3116178)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6136

[Update Details](#)

Recommendation is updated

**19397 - (MS15-124) Cumulative Security Update for Internet Explorer (3116180)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6083, CVE-2015-6134, CVE-2015-6135, CVE-2015-6136, CVE-2015-6138, CVE-2015-6139, CVE-2015-6140, CVE-2015-6141, CVE-2015-6142, CVE-2015-6143, CVE-2015-6144, CVE-2015-6145, CVE-2015-6146, CVE-2015-6147, CVE-2015-6148, CVE-2015-6149, CVE-2015-6150, CVE-2015-6151, CVE-2015-6152, CVE-2015-6153, CVE-2015-6154, CVE-2015-6155, CVE-2015-6156, CVE-2015-6157, CVE-2015-6158, CVE-2015-6159, CVE-2015-6160, CVE-2015-6161, CVE-2015-6162, CVE-2015-6164

[Update Details](#)

Recommendation is updated

**19398 - (MS15-126) Cumulative Security Update for JScript and VBScript to Address Remote Code Execution (3116178)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6135, CVE-2015-6136

[Update Details](#)

Recommendation is updated

**19402 - (MS15-125) Microsoft Edge Memory Corruption Remote Code Execution I (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6140

[Update Details](#)

Recommendation is updated

**19404 - (MS15-125) Microsoft Edge Memory Corruption Remote Code Execution II (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6142

[Update Details](#)

Recommendation is updated

**19405 - (MS15-125) Microsoft Edge Memory Corruption Remote Code Execution III (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6148

[Update Details](#)

Recommendation is updated

**19406 - (MS15-125) Microsoft Edge Memory Corruption Remote Code Execution IV (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6151

[Update Details](#)

Recommendation is updated

**19407 - (MS15-125) Microsoft Edge Memory Corruption Remote Code Execution V (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6153

[Update Details](#)

Recommendation is updated

**19408 - (MS15-125) Microsoft Edge Memory Corruption Remote Code Execution VI (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6154

[Update Details](#)

Recommendation is updated

**19409 - (MS15-125) Microsoft Edge Memory Corruption Remote Code Execution VII (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6155

[Update Details](#)

Recommendation is updated

**19410 - (MS15-125) Microsoft Edge Memory Corruption Remote Code Execution VIII (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6158

[Update Details](#)

Recommendation is updated

**19411 - (MS15-125) Microsoft Edge Memory Corruption Remote Code Execution IX (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6159

[Update Details](#)

Recommendation is updated

**19413 - (MS15-125) Microsoft Edge Memory Corruption Remote Code Execution X (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6168

[Update Details](#)

Recommendation is updated

**19417 - (MS15-125) Cumulative Security Update for Microsoft Edge (3116184)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6139, CVE-2015-6140, CVE-2015-6142, CVE-2015-6148, CVE-2015-6151, CVE-2015-6153, CVE-2015-6154, CVE-2015-6155, CVE-2015-6158, CVE-2015-6159, CVE-2015-6161, CVE-2015-6168, CVE-2015-6169, CVE-2015-6170, CVE-2015-6176

[Update Details](#)

Recommendation is updated

**19418 - (MS15-129) Microsoft Silverlight Remote Code Execution (3106614)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6166

[Update Details](#)

Recommendation is updated

#### **19421 - (MS15-129) Multiple Vulnerabilities in Silverlight Could Allow Remote Code Execution (3106614)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6114, CVE-2015-6165, CVE-2015-6166

#### Update Details

Recommendation is updated

#### **19422 - (MS15-129) Multiple Vulnerabilities in Silverlight Could Allow Remote Code Execution (3106614)**

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2015-6114, CVE-2015-6165, CVE-2015-6166

#### Update Details

Recommendation is updated

#### **19505 - (MS16-002) Cumulative Security Update for Microsoft Edge (3124904)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0003, CVE-2016-0024

#### Update Details

Recommendation is updated

#### **19506 - (MS16-002) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution (3124904)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0024

#### Update Details

Recommendation is updated

#### **19507 - (MS16-002) Microsoft Edge Memory Corruption Remote Code Execution (3124904)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0003

#### Update Details

Recommendation is updated

### 19508 - (MS16-005) Security Update for Windows Kernel-Mode Drivers to Address Remote Code Execution (3124584)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0008, CVE-2016-0009

#### Update Details

Recommendation is updated

### 19509 - (MS16-005) Microsoft Windows Win32k Remote Code Execution (3124584)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0009

#### Update Details

Recommendation is updated

### 19511 - (MS16-006) Security Update for Silverlight to Address Remote Code Execution (3126036)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0034

#### Update Details

Recommendation is updated

### 19512 - (MS16-006) Microsoft Silverlight Runtime Remote Code Execution (3126036)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0034

#### Update Details

Recommendation is updated

### 19523 - (MS16-001) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution (3124903)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0002

#### Update Details

Recommendation is updated

### 19526 - (MS16-004) Microsoft Office Memory Corruption Remote Code Execution I (3124585)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0010

Update Details

Recommendation is updated

**19530 - (MS16-004) Microsoft Office Memory Corruption Remote Code Execution II (3124585)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0035

Update Details

Recommendation is updated

**19531 - (MS16-001) Cumulative Security Update for Internet Explorer (3124903)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0002, CVE-2016-0005

Update Details

Recommendation is updated

**19533 - (MS16-004) Security Update for Microsoft Office to Address Remote Code Execution (3124585)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6117, CVE-2016-0010, CVE-2016-0011, CVE-2016-0012, CVE-2016-0035

Update Details

Recommendation is updated

**19534 - (MS16-006) Security Update for Silverlight to Address Remote Code Execution (3126036)**

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-0034

Update Details

Recommendation is updated

**19549 - (MS16-004) Security Update for Microsoft Office to Address Remote Code Execution (3124585)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2015-6117, CVE-2016-0010, CVE-2016-0011, CVE-2016-0012, CVE-2016-0035

Update Details

Recommendation is updated

**19619 - (MS16-011) Microsoft Edge Memory Corruption Remote Code Execution IV (3134225)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0084

Update Details

Recommendation is updated

**19624 - (MS16-011) Microsoft Edge Memory Corruption Remote Code Execution II (3134225)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0062

Update Details

Recommendation is updated

**19625 - (MS16-011) Microsoft Edge Memory Corruption Remote Code Execution I (3134225)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0061

Update Details

Recommendation is updated

**19626 - (MS16-015) Security Update for Microsoft Office to Address Remote Code Execution (3134226)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0022, CVE-2016-0039, CVE-2016-0052, CVE-2016-0053, CVE-2016-0054, CVE-2016-0055, CVE-2016-0056, CVE-2016-0057

Update Details

Recommendation is updated

**19627 - (MS16-015) Security Update for Microsoft Office to Address Remote Code Execution (3134226)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-0022, CVE-2016-0039, CVE-2016-0052, CVE-2016-0053, CVE-2016-0054, CVE-2016-0055, CVE-2016-0056, CVE-2016-0057



[Update Details](#)

Recommendation is updated

**19630 - (MS16-015) Microsoft Office Memory Corruption Remote Code Execution VI (3134226)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0056

[Update Details](#)

Recommendation is updated

**19631 - (MS16-015) Microsoft Office Memory Corruption Remote Code Execution V (3134226)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0055

[Update Details](#)

Recommendation is updated

**19632 - (MS16-015) Microsoft Office Memory Corruption Remote Code Execution IV (3134226)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0054

[Update Details](#)

Recommendation is updated

**19633 - (MS16-015) Microsoft Office Memory Corruption Remote Code Execution III (3134226)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0053

[Update Details](#)

Recommendation is updated

**19634 - (MS16-015) Microsoft Office Memory Corruption Remote Code Execution II (3134226)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0052

[Update Details](#)

Recommendation is updated

#### **19635 - (MS16-015) Microsoft Office Memory Corruption Remote Code Execution I (3134226)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0022

##### Update Details

Recommendation is updated

#### **19636 - (MS16-011) Cumulative Security Update for Microsoft Edge (3134225)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0060, CVE-2016-0061, CVE-2016-0062, CVE-2016-0077, CVE-2016-0080, CVE-2016-0084

##### Update Details

Recommendation is updated

#### **19641 - (MS16-009) Microsoft Internet Explorer Memory Corruption Remote Code Execution VIII (3134220)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0072

##### Update Details

Recommendation is updated

#### **19642 - (MS16-009) Microsoft Internet Explorer Memory Corruption Remote Code Execution VII (3134220)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0071

##### Update Details

Recommendation is updated

#### **19643 - (MS16-009) Microsoft Internet Explorer Cross-Domain Policies Privilege Escalation II (3134220)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0069

##### Update Details

Recommendation is updated

---

#### 19644 - (MS16-009) Microsoft Internet Explorer Cross-Domain Policies Privilege Escalation I (3134220)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0068

##### Update Details

Recommendation is updated

#### 19645 - (MS16-009) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3134220)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0067

##### Update Details

Recommendation is updated

#### 19649 - (MS16-009) Microsoft Internet Explorer Memory Corruption Remote Code Execution VI (3134220)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0064

##### Update Details

Recommendation is updated

#### 19650 - (MS16-009) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3134220)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0063

##### Update Details

Recommendation is updated

#### 19651 - (MS16-009) Microsoft Internet Explorer Browser Memory Corruption Remote Code Execution III (3134220)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0062

##### Update Details

Recommendation is updated

#### 19652 - (MS16-009) Microsoft Internet Explorer Browser Memory Corruption Remote Code Execution II (3134220)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0061

Update Details

Recommendation is updated

**19653 - (MS16-009) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3134220)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0060

Update Details

Recommendation is updated

**19655 - (MS16-009) Cumulative Security Update for Internet Explorer (3134220)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0041, CVE-2016-0059, CVE-2016-0060, CVE-2016-0061, CVE-2016-0062, CVE-2016-0063, CVE-2016-0064, CVE-2016-0067, CVE-2016-0068, CVE-2016-0069, CVE-2016-0071, CVE-2016-0072, CVE-2016-0077

Update Details

Recommendation is updated

**19663 - (MS16-013) Microsoft Windows Journal File Parsing TIFFControl Invalid Reference Remote Code Execution (3134811)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0038

Update Details

Recommendation is updated

**19672 - (MS16-013) Security Update for Windows Journal to Address Remote Code Execution (3134811)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0038

Update Details

Recommendation is updated

**19680 - (MS16-009) Microsoft Internet Explorer HTTP Parsing Spoofing Information Disclosure (3134220)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0077

Update Details

Recommendation is updated

**19734 - (MS16-029) Security Update for Microsoft Office to Address Remote Code Execution (3141806)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0021, CVE-2016-0057, CVE-2016-0134

Update Details

Recommendation is updated

**19735 - (MS16-029) Security Update for Microsoft Office to Address Remote Code Execution (3141806)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-0021, CVE-2016-0057, CVE-2016-0134

Update Details

Recommendation is updated

**19741 - (MS16-027) Security Update for Windows Media to Address Remote Code Execution (3143146)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0098, CVE-2016-0101

Update Details

Recommendation is updated

**19742 - (MS16-027) Microsoft Windows Media Player Parsing Remote Code Execution II (3143146)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0101

Update Details

Recommendation is updated

**19743 - (MS16-027) Microsoft Windows Media Player Parsing Remote Code Execution I (3143146)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0098

Update Details

Recommendation is updated

**19744 - (MS16-028) Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3143081)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0117, CVE-2016-0118

Update Details

Recommendation is updated

**19745 - (MS16-028) Microsoft Windows PDF Library Remote Code Execution II (3143081)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0118

Update Details

Recommendation is updated

**19746 - (MS16-028) Microsoft Windows PDF Library Remote Code Execution I (3143081)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0117

Update Details

Recommendation is updated

**19750 - (MS16-024) Microsoft Edge Memory Corruption Remote Code Execution I (3142019)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0102

Update Details

Recommendation is updated

**19753 - (MS16-024) Microsoft Edge Memory Corruption Remote Code Execution II (3142019)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0105

[Update Details](#)

Recommendation is updated

**19756 - (MS16-024) Microsoft Edge Memory Corruption Remote Code Execution III (3142019)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0109

[Update Details](#)

Recommendation is updated

**19758 - (MS16-024) Microsoft Edge Memory Corruption Remote Code Execution IV (3142019)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0110

[Update Details](#)

Recommendation is updated

**19759 - (MS16-024) Microsoft Edge Memory Corruption Remote Code Execution V (3142019)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0111

[Update Details](#)

Recommendation is updated

**19760 - (MS16-024) Microsoft Edge Memory Corruption Remote Code Execution VI (3142019)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0116

[Update Details](#)

Recommendation is updated

**19765 - (MS16-024) Microsoft Edge Memory Corruption Remote Code Execution VII (3142019)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0123

[Update Details](#)

Recommendation is updated

#### **19766 - (MS16-024) Microsoft Edge Memory Corruption Remote Code Execution VIII (3142019)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0124

[Update Details](#)

Recommendation is updated

#### **19768 - (MS16-024) Microsoft Edge Memory Corruption Remote Code Execution IX (3142019)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0129

[Update Details](#)

Recommendation is updated

#### **19769 - (MS16-024) Microsoft Edge Memory Corruption Remote Code Execution X (3142019)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0130

[Update Details](#)

Recommendation is updated

#### **19771 - (MS16-023) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3142015)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0104

[Update Details](#)

Recommendation is updated

#### **19772 - (MS16-023) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3142015)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0102

[Update Details](#)

Recommendation is updated

---



### 19773 - (MS16-023) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3142015)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0103

#### Update Details

Recommendation is updated

### 19774 - (MS16-023) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3142015)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0105

#### Update Details

Recommendation is updated

### 19775 - (MS16-023) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3142015)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0106

#### Update Details

Recommendation is updated

### 19776 - (MS16-023) Microsoft Internet Explorer Memory Corruption Remote Code Execution VI (3142015)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0107

#### Update Details

Recommendation is updated

### 19777 - (MS16-023) Microsoft Internet Explorer Memory Corruption Remote Code Execution VII (3142015)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0108

#### Update Details

Recommendation is updated

### 19778 - (MS16-023) Microsoft Internet Explorer Memory Corruption Remote Code Execution VIII (3142015)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0109

Update Details

Recommendation is updated

**19779 - (MS16-023) Microsoft Internet Explorer Memory Corruption Remote Code Execution IX (3142015)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0110

Update Details

Recommendation is updated

**19780 - (MS16-023) Microsoft Internet Explorer Memory Corruption Remote Code Execution X (3142015)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0111

Update Details

Recommendation is updated

**19781 - (MS16-023) Microsoft Internet Explorer Memory Corruption Remote Code Execution XI (3142015)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0112

Update Details

Recommendation is updated

**19782 - (MS16-023) Microsoft Internet Explorer Memory Corruption Remote Code Execution XII (3142015)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0113

Update Details

Recommendation is updated

**19783 - (MS16-023) Microsoft Internet Explorer Memory Corruption Remote Code Execution XIII (3142015)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0114

Update Details

Recommendation is updated

**19784 - (MS16-030) Security Update for Windows OLE to Address Remote Code Execution (3143136)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0091, CVE-2016-0092

Update Details

Recommendation is updated

**19789 - (MS16-026) Security Update for Graphic Fonts to Address Remote Code Execution (3143148)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0120, CVE-2016-0121

Update Details

Recommendation is updated

**19791 - (MS16-026) Microsoft Windows Adobe Type Manager Library OpenFont Parsing Remote Code Execution (3143148)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0121

Update Details

Recommendation is updated

**19899 - (MS16-039) Security Update for Microsoft Graphics Component (3148522)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0143, CVE-2016-0145, CVE-2016-0165, CVE-2016-0167

Update Details

Recommendation is updated

**19909 - (MS16-039) Microsoft Windows Win32k Graphics Privilege Escalation III (3148522)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0167

[Update Details](#)

Recommendation is updated

**19910 - (MS16-039) Microsoft Windows Graphics Memory Remote Code Execution (3148522)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0145

[Update Details](#)

Recommendation is updated

**19911 - (MS16-038) Microsoft Edge Memory Corruption Remote Code Execution I (3148532)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0154

[Update Details](#)

Recommendation is updated

**19912 - (MS16-038) Microsoft Edge Memory Corruption Remote Code Execution II (3148532)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0155

[Update Details](#)

Recommendation is updated

**19913 - (MS16-038) Microsoft Edge Memory Corruption Remote Code Execution III (3148532)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0156

[Update Details](#)

Recommendation is updated

**19914 - (MS16-038) Microsoft Edge Memory Corruption Remote Code Execution IV (3148532)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0157

[Update Details](#)

Recommendation is updated

### 19915 - (MS16-038) Microsoft Edge Cross Domain Privilege Escalation (3148532)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0158

#### Update Details

Recommendation is updated

### 19925 - (MS16-042) Security Update for Microsoft Office (3148775)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0122, CVE-2016-0127, CVE-2016-0136, CVE-2016-0139

#### Update Details

Recommendation is updated

### 19926 - (MS16-042) Security Update for Microsoft Office (3148775)

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-0122, CVE-2016-0127, CVE-2016-0136, CVE-2016-0139

#### Update Details

Recommendation is updated

### 19930 - (MS16-042) Microsoft Office Memory Corruption Remote Code Execution II (3148775)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0127

#### Update Details

Recommendation is updated

### 19932 - (MS16-040) Microsoft Windows MSXML Remote Code Execution (3148541)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0147

#### Update Details

Recommendation is updated

### 19936 - (MS16-040) Security Update for Microsoft XML Core Services (3148541)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0147

#### Update Details

Recommendation is updated

### 19938 - (MS16-037) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3148531)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0154

#### Update Details

Recommendation is updated

### 19939 - (MS16-037) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3148531)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0159

#### Update Details

Recommendation is updated

### 19940 - (MS16-037) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3148531)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0160

#### Update Details

Recommendation is updated

### 19942 - (MS16-037) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3148531)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0164

#### Update Details

Recommendation is updated

### 19943 - (MS16-037) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3148531)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0166

Update Details

Recommendation is updated

**20006 - (MS16-061) Security Update for Microsoft RPC (3155520)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0178

Update Details

Recommendation is updated

**20008 - (MS16-061) Microsoft Windows Remote Procedure Call NDR Engine Privilege Escalation (3155520)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0178

Update Details

Recommendation is updated

**20010 - (MS16-051) Cumulative Security Update for Internet Explorer (3155533)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0187, CVE-2016-0188, CVE-2016-0189, CVE-2016-0192, CVE-2016-0194

Update Details

Recommendation is updated

**20012 - (MS16-051) Microsoft Internet Explorer Security Bypass (3155533)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0188

Update Details

Recommendation is updated

**20016 - (MS16-055) Security Update for Microsoft Graphics Component (3156754)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0168, CVE-2016-0169, CVE-2016-0170, CVE-2016-0184, CVE-2016-0195

Update Details

Recommendation is updated

**20019 - (MS16-055) Microsoft Windows Graphics Remote Code Execution (3156754)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0170

Update Details

Recommendation is updated

**20020 - (MS16-055) Microsoft Windows Graphics Direct3D Remote Code Execution (3156754)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0184

Update Details

Recommendation is updated

**20021 - (MS16-055) Microsoft Windows Graphics Imaging Component Remote Code Execution (3156754)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0195

Update Details

Recommendation is updated

**20030 - (MS16-054) Microsoft Office Memory Corruption Remote Code Execution I (3155544)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0126

Update Details

Recommendation is updated

**20031 - (MS16-054) Microsoft Office Memory Corruption Remote Code Execution II (3155544)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0140



Update Details

Recommendation is updated

**20032 - (MS16-054) Microsoft Office Memory Corruption Remote Code Execution III (3155544)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0198

Update Details

Recommendation is updated

**20033 - (MS16-054) Microsoft Office Graphics Remote Code Execution (3155544)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0183

Update Details

Recommendation is updated

**20046 - (MS16-054) Security Update for Microsoft Office (3155544)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0126, CVE-2016-0140, CVE-2016-0183, CVE-2016-0198

Update Details

Recommendation is updated

**20051 - (MS16-056) Microsoft Windows Journal Memory Corruption Remote Code Execution (3156761)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0182

Update Details

Recommendation is updated

**20052 - (MS16-056) Security Update for Windows Journal (3156761)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0182

Update Details

Recommendation is updated

#### **20056 - (MS16-057) Microsoft Windows Shell Remote Code Execution (3156987)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0179

#### Update Details

Recommendation is updated

#### **20057 - (MS16-057) Security Update for Windows Shell (3156987)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0179

#### Update Details

Recommendation is updated

#### **20070 - (MS16-054) Security Update for Microsoft Office (3155544)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-0126, CVE-2016-0140, CVE-2016-0183, CVE-2016-0198

#### Update Details

Recommendation is updated

#### **20145 - (MS16-080) Security Update for Microsoft Windows PDF (3164302)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3201, CVE-2016-3203, CVE-2016-3215

#### Update Details

Recommendation is updated

#### **20150 - (MS16-068) Microsoft Edge Chakra Scripting Engine Memory Corruption Remote Code Execution I (3163656)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3199

#### Update Details

Recommendation is updated

### 20153 - (MS16-068) Microsoft Edge PDF Remote Code Execution (3163656)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3203

#### Update Details

Recommendation is updated

### 20154 - (MS16-068) Microsoft Edge Chakra Scripting Engine Memory Corruption Remote Code Execution III (3163656)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3214

#### Update Details

Recommendation is updated

### 20157 - (MS16-068) Cumulative Security Update for Microsoft Edge (3163656)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3198, CVE-2016-3199, CVE-2016-3201, CVE-2016-3202, CVE-2016-3203, CVE-2016-3214, CVE-2016-3215, CVE-2016-3222

#### Update Details

Recommendation is updated

### 20161 - (MS16-070) Microsoft Office Memory Corruption Remote Code Execution I (3163610)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0025

#### Update Details

Recommendation is updated

### 20162 - (MS16-070) Security Update for Microsoft Office (3163610)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0025, CVE-2016-3233, CVE-2016-3234, CVE-2016-3235

#### Update Details

Recommendation is updated

### 20163 - (MS16-070) Security Update for Microsoft Office (3163610)

---

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-0025, CVE-2016-3233, CVE-2016-3234, CVE-2016-3235

Update Details

Recommendation is updated

**20164 - (MS16-063) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3163649)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0199

Update Details

Recommendation is updated

**20256 - (MS16-088) Microsoft Office Memory Corruption Remote Code Execution VI (3170008)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3284

Update Details

Recommendation is updated

**20257 - (MS16-088) Microsoft Office Memory Corruption Remote Code Execution V (3170008)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3283

Update Details

Recommendation is updated

**20258 - (MS16-088) Microsoft Office Memory Corruption Remote Code Execution IV (3170008)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3282

Update Details

Recommendation is updated

**20259 - (MS16-088) Microsoft Office Memory Corruption Remote Code Execution III (3170008)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-3281

[Update Details](#)

Recommendation is updated

**20260 - (MS16-088) Microsoft Office Memory Corruption Remote Code Execution II (3170008)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-3280

[Update Details](#)

Recommendation is updated

**20262 - (MS16-088) Microsoft Office Memory Corruption Remote Code Execution I (3170008)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-3278

[Update Details](#)

Recommendation is updated

**20263 - (MS16-088) Security Updates for Microsoft Office (3170008)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-3278, CVE-2016-3279, CVE-2016-3280, CVE-2016-3281, CVE-2016-3282, CVE-2016-3283, CVE-2016-3284

[Update Details](#)

Recommendation is updated

**20264 - (MS16-088) Security Updates for Microsoft Office (3170008)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High  
CVE: CVE-2016-3278, CVE-2016-3279, CVE-2016-3280, CVE-2016-3281, CVE-2016-3282, CVE-2016-3283, CVE-2016-3284

[Update Details](#)

Recommendation is updated

**20273 - (MS16-087) Microsoft Windows Print Spooler Drivers Remote Code Execution (3170005)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-3238

[Update Details](#)

Recommendation is updated

**20279 - (MS16-087) Security Update for Windows Print Spooler Components (3170005)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3238, CVE-2016-3239

[Update Details](#)

Recommendation is updated

**20286 - (MS16-084) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution IV (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3260

[Update Details](#)

Recommendation is updated

**20287 - (MS16-084) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution III (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3259

[Update Details](#)

Recommendation is updated

**20288 - (MS16-084) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution II (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3248

[Update Details](#)

Recommendation is updated

**20289 - (MS16-084) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution I (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3204

[Update Details](#)

Recommendation is updated

### **20295 - (MS16-085) Cumulative Security Update for Microsoft Edge (3169999)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3244, CVE-2016-3246, CVE-2016-3248, CVE-2016-3259, CVE-2016-3260, CVE-2016-3264, CVE-2016-3265, CVE-2016-3269, CVE-2016-3271, CVE-2016-3273, CVE-2016-3274, CVE-2016-3276, CVE-2016-3277

[Update Details](#)

Recommendation is updated

### **20298 - (MS16-084) Cumulative Security Update for Internet Explorer (3169991)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3204, CVE-2016-3240, CVE-2016-3241, CVE-2016-3242, CVE-2016-3243, CVE-2016-3245, CVE-2016-3248, CVE-2016-3259, CVE-2016-3260, CVE-2016-3261, CVE-2016-3273, CVE-2016-3274, CVE-2016-3276, CVE-2016-3277

[Update Details](#)

Recommendation is updated

### **20303 - (MS16-085) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution V (3169999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3269

[Update Details](#)

Recommendation is updated

### **20304 - (MS16-085) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution IV (3169999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3265

[Update Details](#)

Recommendation is updated

### **20305 - (MS16-085) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution III (3169999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3260

[Update Details](#)

Recommendation is updated

#### **20306 - (MS16-085) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution II (3169999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3259

[Update Details](#)

Recommendation is updated

#### **20307 - (MS16-085) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution I (3169999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3248

[Update Details](#)

Recommendation is updated

#### **20325 - (MS16-085) Microsoft Edge Memory Corruption Remote Code Execution VI (3169999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3264

[Update Details](#)

Recommendation is updated

#### **20374 - (MS16-096) Cumulative Security Update for Microsoft Edge (3177358)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3289, CVE-2016-3293, CVE-2016-3296, CVE-2016-3319, CVE-2016-3322, CVE-2016-3326, CVE-2016-3327, CVE-2016-3329

[Update Details](#)

Recommendation is updated

#### **20381 - (MS16-102) Microsoft Windows PDF Library Remote Code Execution (3182248)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3319

[Update Details](#)

Recommendation is updated



### **20382 - (MS16-099) Security Update for Microsoft Office (3177451)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3313, CVE-2016-3315, CVE-2016-3316, CVE-2016-3317, CVE-2016-3318

#### Update Details

Recommendation is updated

### **20383 - (MS16-099) Security Update for Microsoft Office (3177451)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-3313, CVE-2016-3315, CVE-2016-3316, CVE-2016-3317, CVE-2016-3318

#### Update Details

Recommendation is updated

### **20386 - (MS16-096) Microsoft Edge Browser Memory Corruption Remote Code Execution I (3177358)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3289

#### Update Details

Recommendation is updated

### **20388 - (MS16-096) Microsoft Edge Chakra Javascript Engine Remote Code Execution (3177358)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3296

#### Update Details

Recommendation is updated

### **20390 - (MS16-096) Microsoft Edge Browser Memory Corruption Remote Code Execution (3177358)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3322

#### Update Details

Recommendation is updated

### **20396 - (MS16-101) Microsoft Windows Netlogon Privilege Escalation (3178465)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3300

Update Details

Recommendation is updated

**20402 - (MS16-095) Microsoft Internet Explorer Browser Memory Corruption Remote Code Execution III (3177356)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3322

Update Details

Recommendation is updated

**20404 - (MS16-095) Microsoft Internet Explorer Browser Memory Corruption Remote Code Execution II (3177356)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3293

Update Details

Recommendation is updated

**20405 - (MS16-095) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3177356)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3290

Update Details

Recommendation is updated

**20406 - (MS16-095) Microsoft Internet Explorer Browser Memory Corruption Remote Code Execution I (3177356)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3289

Update Details

Recommendation is updated

**20407 - (MS16-095) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3177356)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3288

[Update Details](#)

Recommendation is updated

**20408 - (MS16-097) Microsoft Windows Graphics Component Remote Code Execution III (3177393)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3304

[Update Details](#)

Recommendation is updated

**20409 - (MS16-097) Microsoft Windows Graphics Component Remote Code Execution II (3177393)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3303

[Update Details](#)

Recommendation is updated

**20410 - (MS16-097) Microsoft Windows Graphics Component Remote Code Execution I (3177393)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3301

[Update Details](#)

Recommendation is updated

**20417 - (MS16-097) Security Update for Microsoft Graphics Component (3177393)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3301, CVE-2016-3303, CVE-2016-3304

[Update Details](#)

Recommendation is updated

**20482 - (MS16-110) Security Update for Microsoft Windows (3178467)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3346, CVE-2016-3352, CVE-2016-3368, CVE-2016-3369

[Update Details](#)

Recommendation is updated

**20501 - (MS16-106) Security Update for Microsoft Graphics Component (3185848)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3348, CVE-2016-3349, CVE-2016-3354, CVE-2016-3355, CVE-2016-3356

[Update Details](#)

Recommendation is updated

**20505 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution II (3183043)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3294

[Update Details](#)

Recommendation is updated

**20506 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution III (3183043)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3295

[Update Details](#)

Recommendation is updated

**20509 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution VI (3183043)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3350

[Update Details](#)

Recommendation is updated

**20510 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution VII (3183043)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3377

[Update Details](#)

Recommendation is updated

#### **20524 - (MS16-106) Microsoft Windows Graphics Component GDI Memory Handling Remote Code Execution (3185848)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3356

[Update Details](#)

Recommendation is updated

#### **20537 - (MS16-104) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3183038)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3295

[Update Details](#)

Recommendation is updated

#### **20543 - (MS16-104) Microsoft Internet Explorer Memory Corruption Remote Code Execution V (3183038)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3375

[Update Details](#)

Recommendation is updated

#### **20545 - (MS16-107) Microsoft Office Memory Corruption Remote Code Execution I (3185852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3357

[Update Details](#)

Recommendation is updated

#### **20555 - (MS16-107) Security Update for Microsoft Office (3185852)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-0141, CVE-2016-3357, CVE-2016-3358, CVE-2016-3359, CVE-2016-3360, CVE-2016-3361, CVE-2016-3362, CVE-2016-3363, CVE-2016-3365, CVE-2016-3366, CVE-2016-3381

[Update Details](#)

Recommendation is updated

### 20556 - (MS16-107) Security Update for Microsoft Office (3185852)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0141, CVE-2016-3357, CVE-2016-3358, CVE-2016-3359, CVE-2016-3360, CVE-2016-3361, CVE-2016-3362, CVE-2016-3363, CVE-2016-3365, CVE-2016-3366, CVE-2016-3381

#### Update Details

Recommendation is updated

### 4576 - (MS06-060) Microsoft Word Malformed Stack Vulnerability (924554)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3647, CVE-2006-3651, CVE-2006-4534 , CVE-2006-4693

#### Update Details

Recommendation is updated

### 4678 - (MS06-060) Microsoft Word Vulnerability (924554)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3647, CVE-2006-3651, CVE-2006-4534, CVE-2006-4693

#### Update Details

Recommendation is updated

### 4680 - (MS06-060) Microsoft Word Mail Merge Vulnerability (924554)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-3647, CVE-2006-3651, CVE-2006-4534, CVE-2006-4693

#### Update Details

Recommendation is updated

### 4780 - (MS07-014) Microsoft Word Malformed String Vulnerability (929434)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5994

#### Update Details

Recommendation is updated

### 4783 - (MS07-014) Microsoft Word Malformed Data Structures Vulnerability (929434)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-6456

[Update Details](#)

Recommendation is updated

**4800 - (MS07-014) Microsoft Word Count Vulnerability (929434)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-6561

[Update Details](#)

Recommendation is updated

**4940 - (MS07-014) Microsoft Word Macro Vulnerability (929434)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5994, CVE-2006-6456, CVE-2006-6561, CVE-2007-0208 , CVE-2007-0209, CVE-2007-0515

[Update Details](#)

Recommendation is updated

**4941 - (MS07-014) Microsoft Word Malformed Drawing Object Vulnerability (929434)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-5994, CVE-2006-6456, CVE-2006-6561, CVE-2007-0208, CVE-2007-0209, CVE-2007-0515

[Update Details](#)

Recommendation is updated

**5124 - (MS07-024) Microsoft RTF Word Parsing Vulnerability (934232)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0035, CVE-2007-0870, CVE-2007-1202

[Update Details](#)

Recommendation is updated

**5137 - (MS07-024) Microsoft Word Document Stream Vulnerability (934232)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-0035, CVE-2007-0870, CVE-2007-1202

[Update Details](#)

Recommendation is updated

#### **5515 - (MS07-058) Microsoft Windows RPC Authentication Vulnerability Could Allow Denial of Service (933729)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-2228

[Update Details](#)

Recommendation is updated

#### **5530 - (MS07-058) Microsoft Windows RPC Authentication Vulnerability Could Allow Denial of Service (933729) - No Credentials Required**

Category: Windows Host Assessment -> No Credentials Required

Risk Level: High

CVE: CVE-2007-2228

[Update Details](#)

Recommendation is updated

#### **6275 - (MS08-072) Microsoft Word RTF Object Parsing Vulnerability IV (957173)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4031

[Update Details](#)

Recommendation is updated

#### **6276 - (MS08-072) Microsoft Word Memory Corruption Vulnerability (957173)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4024

[Update Details](#)

Recommendation is updated

#### **6277 - (MS08-072) Microsoft Word Memory Corruption Vulnerability II (957173)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High



CVE: CVE-2008-4837

[Update Details](#)

Recommendation is updated

**6278 - (MS08-072) Microsoft Word RTF Object Parsing Vulnerability I (957173)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4027

[Update Details](#)

Recommendation is updated

**6279 - (MS08-072) Microsoft Word RTF Object Parsing Vulnerability II (957173)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4030

[Update Details](#)

Recommendation is updated

**6280 - (MS08-072) Microsoft Word RTF Object Parsing Vulnerability III (957173)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4028

[Update Details](#)

Recommendation is updated

**6281 - (MS08-072) Microsoft Word RTF Object Parsing Vulnerability (957173)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4025

[Update Details](#)

Recommendation is updated

**6282 - (MS08-072) Microsoft Word Memory Corruption Remote Code Execution (957173)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4026

[Update Details](#)

Recommendation is updated

**6492 - (MS09-006) Microsoft Windows Kernel Input Validation Vulnerability (958690)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0081

[Update Details](#)

Recommendation is updated

**6771 - (MS09-027) Microsoft Office Word Buffer Overflow Vulnerability (969514)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0563

[Update Details](#)

Recommendation is updated

**6772 - (MS09-027) Microsoft Office Word Buffer Overflow Vulnerability II (969514)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0565

[Update Details](#)

Recommendation is updated

**7546 - (MS09-027) Vulnerabilities In Microsoft Office Word Could Allow Remote Code Execution (969514)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-0563, CVE-2009-0565

[Update Details](#)

Recommendation is updated

**8298 - (MS08-072) Vulnerabilities In Microsoft Office Word Could Allow Remote Code Execution (957173)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-4024, CVE-2008-4025, CVE-2008-4026, CVE-2008-4027, CVE-2008-4028, CVE-2008-4030, CVE-2008-4031, CVE-2008-4837

[Update Details](#)

Recommendation is updated

#### **12250 - (MS11-042) Vulnerabilities In Distributed File System Could Allow Remote Code Execution (2535512)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1868, CVE-2011-1869

#### Update Details

Recommendation is updated

#### **12348 - (MS11-056) Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2507938)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1281, CVE-2011-1282, CVE-2011-1283, CVE-2011-1284, CVE-2011-1870

#### Update Details

Recommendation is updated

#### **13292 - (MS12-008) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-5046, CVE-2012-0154

#### Update Details

Recommendation is updated

#### **13552 - (MS09-027) Vulnerabilities In Microsoft Office Word Could Allow Remote Code Execution (969514)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2009-0563, CVE-2009-0565

#### Update Details

Recommendation is updated

#### **13780 - (MS12-042) Microsoft Windows BIOS ROM Corruption Privilege Escalation (2711167)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1515

#### Update Details

Recommendation is updated

### 13787 - (MS12-042) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2711167)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0217, CVE-2012-1515

#### Update Details

Recommendation is updated

### 14210 - (MS12-064) Vulnerabilities In Microsoft Word Could Allow Remote Code Execution (2742319)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0182, CVE-2012-2528

#### Update Details

Recommendation is updated

### 16566 - (MS14-021) Security Update for Internet Explorer (2965111)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-1776

#### Update Details

Recommendation is updated

### 20192 - (MS16-063) Cumulative Security Update for Internet Explorer (3163649)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0199, CVE-2016-0200, CVE-2016-3202, CVE-2016-3205, CVE-2016-3206, CVE-2016-3207, CVE-2016-3210, CVE-2016-3211, CVE-2016-3212, CVE-2016-3213

#### Update Details

Recommendation is updated

### 4390 - (MS06-027) Microsoft Word Code Execution Vulnerability (917336)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2006-2492

#### Update Details

Recommendation is updated

### 5626 - (MS07-066) Microsoft Windows Kernel Vulnerability (943078)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2007-5350

[Update Details](#)

Recommendation is updated

#### **5805 - (MS08-025) Microsoft Windows Kernel Vulnerability (941693)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1084

[Update Details](#)

Recommendation is updated

#### **7227 - (MS09-058) Vulnerabilities In Windows Kernel Could Allow Elevation of Privilege (971486)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2515, CVE-2009-2516, CVE-2009-2517

[Update Details](#)

Recommendation is updated

#### **7316 - (MS09-065) Win32k NULL Pointer Dereferencing Vulnerability (969947)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-1127

[Update Details](#)

Recommendation is updated

#### **7317 - (MS09-065) Win32k Insufficient Data Validation Vulnerability (969947)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2009-2513

[Update Details](#)

Recommendation is updated

#### **7681 - (MS08-061) Vulnerabilities In Windows Kernel Could Allow Elevation Of Privilege (954211)**

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-2250, CVE-2008-2251, CVE-2008-2252

[Update Details](#)

Recommendation is updated

### **7732 - (MS08-025) Vulnerability In Windows Kernel Could Allow Elevation Of Privilege (941693)**

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2008-1084

[Update Details](#)

Recommendation is updated

### **7860 - (MS10-015) Windows Kernel Exception Handler Vulnerability (977165)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0232

[Update Details](#)

Recommendation is updated

### **7861 - (MS10-015) Windows Kernel Double Free Vulnerability (977165)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0233

[Update Details](#)

Recommendation is updated

### **7889 - (MS10-015) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165)**

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0232, CVE-2010-0233

[Update Details](#)

Recommendation is updated

### **8545 - (MS10-021) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)**

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-0234, CVE-2010-0235, CVE-2010-0236, CVE-2010-0237, CVE-2010-0238, CVE-2010-0481, CVE-2010-0482, CVE-2010-0810

Update Details

Recommendation is updated

**9694 - (MS10-048) Microsoft Windows Win32k Window Creation Vulnerability (2160329)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1897

Update Details

Recommendation is updated

**9695 - (MS10-048) Microsoft Windows Win32k User Input Validation Vulnerability (2160329)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1896

Update Details

Recommendation is updated

**9696 - (MS10-048) Microsoft Windows Win32k Exception Handling Vulnerability (2160329)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1894

Update Details

Recommendation is updated

**9715 - (MS10-047) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1888, CVE-2010-1889, CVE-2010-1890

Update Details

Recommendation is updated

**9722 - (MS10-048) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-1887, CVE-2010-1894, CVE-2010-1895, CVE-2010-1896, CVE-2010-1897

[Update Details](#)

Recommendation is updated

**10317 - (MS10-085) Vulnerability in SChannel Could Allow Denial of Service (2207566)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3229

[Update Details](#)

Recommendation is updated

**10318 - (MS10-085) Microsoft Windows TLSv1 Denial of Service (2207566)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3229

[Update Details](#)

Recommendation is updated

**10773 - (MS11-011) Windows Kernel Improper Data Validation (2393802)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-4398

[Update Details](#)

Recommendation is updated

**10869 - (MS10-098) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3939, CVE-2010-3940, CVE-2010-3941, CVE-2010-3942, CVE-2010-3943, CVE-2010-3944

[Update Details](#)

Recommendation is updated

**10898 - (MS10-098) Microsoft Windows Win32k Buffer Overflow Could Allow Elevation Of Privilege (2436673)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-2739, CVE-2010-3939

[Update Details](#)



Recommendation is updated

**10899 - (MS10-098) Microsoft Windows Win32k Buffer Overflow Could Allow Elevation Of Privilege CVE-2010-3940 (2436673)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3940

[Update Details](#)

Recommendation is updated

**10900 - (MS10-098) Microsoft Windows Win32k Double Free Could Allow Elevation Of Privilege (2436673)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3941

[Update Details](#)

Recommendation is updated

**10901 - (MS10-098) Microsoft Windows Win32k WriteAV Could Allow Elevation Of Privilege (2436673)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3942

[Update Details](#)

Recommendation is updated

**10902 - (MS10-098) Microsoft Windows Win32k Cursor Linking Could Allow Elevation Of Privilege (2436673)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3943

[Update Details](#)

Recommendation is updated

**10903 - (MS10-098) Microsoft Windows Win32k Memory Corruption Could Allow Elevation Of Privilege (2436673)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-3944

[Update Details](#)

Recommendation is updated

### 11224 - (MS11-013) Microsoft Kerberos Unkeyed Checksum (2496930)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0043

#### Update Details

Recommendation is updated

### 11226 - (MS11-013) Vulnerabilities in Microsoft Kerberos Could Allow Elevation Of Privilege (2496930)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0043, CVE-2011-0091

#### Update Details

Recommendation is updated

### 11237 - (MS11-011) Windows Kernel Integer Truncation (2393802)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0045

#### Update Details

Recommendation is updated

### 11244 - (MS11-012) Microsoft Win32k Improper User Input Validation (2479628)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0086

#### Update Details

Recommendation is updated

### 11245 - (MS11-012) Microsoft Win32k Insufficient User Input Validation (2479628)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0087

#### Update Details

Recommendation is updated

### 11246 - (MS11-012) Microsoft Win32k Window Class Pointer Confusion (2479628)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0088

[Update Details](#)

Recommendation is updated

#### **11247 - (MS11-012) Microsoft Win32k Window Class Improper Pointer Validation (2479628)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0089

[Update Details](#)

Recommendation is updated

#### **11248 - (MS11-012) Microsoft Win32k Memory Corruption (2479628)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0090

[Update Details](#)

Recommendation is updated

#### **11253 - (MS11-011) Vulnerabilities In Windows Kernel Could Allow Elevation Of Privilege (2393802)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2010-4398, CVE-2011-0045

[Update Details](#)

Recommendation is updated

#### **11266 - (MS11-012) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Elevation Of Privilege (2479628)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0086, CVE-2011-0087, CVE-2011-0088, CVE-2011-0089, CVE-2011-0090

[Update Details](#)

Recommendation is updated

#### **11791 - (MS11-034) Microsoft Win32k Use After Free I (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0662

[Update Details](#)

Recommendation is updated

#### **11792 - (MS11-034) Microsoft Win32k Use After Free II (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0665

[Update Details](#)

Recommendation is updated

#### **11793 - (MS11-034) Microsoft Win32k Use After Free III (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0666

[Update Details](#)

Recommendation is updated

#### **11794 - (MS11-034) Microsoft Win32k Use After Free IV (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0667

[Update Details](#)

Recommendation is updated

#### **11795 - (MS11-034) Microsoft Win32k Use After Free V (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0670

[Update Details](#)

Recommendation is updated

#### **11796 - (MS11-034) Microsoft Win32k Use After Free VI (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0671

Update Details

Recommendation is updated

**11797 - (MS11-034) Microsoft Win32k Use After Free VII (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0672

Update Details

Recommendation is updated

**11798 - (MS11-034) Microsoft Win32k Use After Free VIII (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0674

Update Details

Recommendation is updated

**11799 - (MS11-034) Microsoft Win32k Use After Free IX (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1234

Update Details

Recommendation is updated

**11800 - (MS11-034) Microsoft Win32k Use After Free X (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1235

Update Details

Recommendation is updated

**11801 - (MS11-034) Microsoft Win32k Use After Free XI (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1236

[Update Details](#)

Recommendation is updated

**11802 - (MS11-034) Microsoft Win32k Use After Free XII (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1237

[Update Details](#)

Recommendation is updated

**11803 - (MS11-034) Microsoft Win32k Use After Free XIII (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1238

[Update Details](#)

Recommendation is updated

**11804 - (MS11-034) Microsoft Win32k Use After Free XIV (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1239

[Update Details](#)

Recommendation is updated

**11805 - (MS11-034) Microsoft Win32k Use After Free XV (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1240

[Update Details](#)

Recommendation is updated

**11806 - (MS11-034) Microsoft Win32k Use After Free XVI (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1241

[Update Details](#)

Recommendation is updated

#### **11807 - (MS11-034) Microsoft Win32k Use After Free XVII (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1242

[Update Details](#)

Recommendation is updated

#### **11808 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation I (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0673

[Update Details](#)

Recommendation is updated

#### **11809 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation II (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0676

[Update Details](#)

Recommendation is updated

#### **11810 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation III (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0677

[Update Details](#)

Recommendation is updated

#### **11811 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation IV (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1225

[Update Details](#)

Recommendation is updated

---

### 11812 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation V (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1226

#### Update Details

Recommendation is updated

### 11813 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation VI (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1227

#### Update Details

Recommendation is updated

### 11814 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation VII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1228

#### Update Details

Recommendation is updated

### 11815 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation VIII (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1229

#### Update Details

Recommendation is updated

### 11816 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation IX (2506223)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1230

#### Update Details

Recommendation is updated

### 11817 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation X (2506223)



Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1231

Update Details

Recommendation is updated

**11818 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation XI (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1232

Update Details

Recommendation is updated

**11819 - (MS11-034) Microsoft Win32k Null Pointer Dereference Privilege Escalation XII (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1233

Update Details

Recommendation is updated

**11836 - (MS11-034) Microsoft Win32k Use After Free XVIII (2506223)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-0675

Update Details

Recommendation is updated

**12222 - (MS11-042) Microsoft Windows DFS Referral Response Denial Of Service (KB2535512)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1869

Update Details

Recommendation is updated

**12324 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation I (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1874

Update Details

Recommendation is updated

**12325 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation II (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1875

Update Details

Recommendation is updated

**12326 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation III (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1876

Update Details

Recommendation is updated

**12327 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation IV (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1877

Update Details

Recommendation is updated

**12328 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation V (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1878

Update Details

Recommendation is updated

**12329 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation VI (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1879

[Update Details](#)

Recommendation is updated

**12330 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation I (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1880

[Update Details](#)

Recommendation is updated

**12331 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation II (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1881

[Update Details](#)

Recommendation is updated

**12332 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation VII (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1882

[Update Details](#)

Recommendation is updated

**12333 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation VIII (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1883

[Update Details](#)

Recommendation is updated

**12334 - (MS11-054) Microsoft Windows Win32k Use After Free Privilege Escalation IX (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1884

[Update Details](#)

Recommendation is updated

#### **12335 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation III (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1885

[Update Details](#)

Recommendation is updated

#### **12337 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation IV (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1887

[Update Details](#)

Recommendation is updated

#### **12338 - (MS11-054) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation V (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1888

[Update Details](#)

Recommendation is updated

#### **12341 - (MS11-056) Microsoft Windows CSRSS Local EOP AllocConsole Privilege Escalation (2507938)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1281

[Update Details](#)

Recommendation is updated

#### **12342 - (MS11-054) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2555917)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1874, CVE-2011-1875, CVE-2011-1876, CVE-2011-1877, CVE-2011-1878, CVE-2011-1879, CVE-2011-1880, CVE-2011-1881, CVE-2011-1882, CVE-2011-1883, CVE-2011-1884, CVE-2011-1885, CVE-2011-1886, CVE-2011-1887, CVE-2011-1888

[Update Details](#)

Recommendation is updated

**12343 - (MS11-056) Microsoft Windows CSRSS Local EOP SrvSetConsoleLocalEUDC Privilege Escalation (2507938)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1282

Update Details

Recommendation is updated

**12344 - (MS11-056) Microsoft Windows CSRSS Local EOP SrvSetConsoleNumberOfCommand Privilege Escalation (2507938)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1283

Update Details

Recommendation is updated

**12345 - (MS11-056) Microsoft Windows CSRSS Local EOP SrvWriteConsoleOutput Privilege Escalation (2507938)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1284

Update Details

Recommendation is updated

**12346 - (MS11-056) Microsoft Windows CSRSS Local EOP SrvWriteConsoleOutputString Privilege Escalation (2507938)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1870

Update Details

Recommendation is updated

**12444 - (MS11-063) Microsoft WCRSS Could Allow Elevation Of Privilege (2567680)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1967

Update Details

Recommendation is updated

**12445 - (MS11-063) Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2567680)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1967

Update Details

Recommendation is updated

**12738 - (MS11-077) Microsoft Windows Kernel-Mode Drivers Win32k Null Pointer De-reference (2567053)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1985

Update Details

Recommendation is updated

**12741 - (MS11-077) Microsoft Windows Kernel-Mode Drivers Win32k Use After Free (2567053)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2011

Update Details

Recommendation is updated

**12913 - (MS11-084) Microsoft Windows TrueType Font Parsing Denial of Service (2617657)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2004

Update Details

Recommendation is updated

**12914 - (MS11-084) Vulnerability in Microsoft Windows Kernel-Mode Drivers Could Allow Denial of Service (2617657)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2004

Update Details

Recommendation is updated

**13055 - (MS11-097) Microsoft Windows CSRSS Local Privilege Elevation (2620712)**

---

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3408

Update Details

Recommendation is updated

**13056 - (MS11-098) Microsoft Windows Kernel Exception Handler (2633171)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2018

Update Details

Recommendation is updated

**13059 - (MS11-097) Vulnerability in Windows Client/Server Runtime Subsystem Could Allow Elevation of Privilege (2620712)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-3408

Update Details

Recommendation is updated

**13060 - (MS11-098) Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2633171)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-2018

Update Details

Recommendation is updated

**13291 - (MS12-008) Microsoft Windows Keyboard Layout Use After Free (2660465)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0154

Update Details

Recommendation is updated

**13396 - (MS12-018) Microsoft Windows PostMessage Function Elevation of Privilege (2641653)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0157

[Update Details](#)

Recommendation is updated

### **13399 - (MS12-018) Vulnerability In Windows Kernel-Mode Drivers Could Allow Elevation Of Privilege (2641653)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0157

[Update Details](#)

Recommendation is updated

### **13626 - (MS12-034) Microsoft Windows Scrollbar Calculation Privilege Escalation (2681578)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1848

[Update Details](#)

Recommendation is updated

### **13627 - (MS12-034) Microsoft Windows Keyboard Layout Privilege Escalation (2681578)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0181

[Update Details](#)

Recommendation is updated

### **13628 - (MS12-034) Microsoft Windows And Messages Privilege Escalation (2681578)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0180

[Update Details](#)

Recommendation is updated

### **13751 - (MS12-041) Microsoft Windows Clipboard Format Atom Name Handling Privilege Escalation (2709162)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High



CVE: CVE-2012-1866

[Update Details](#)

Recommendation is updated

**13776 - (MS12-041) Microsoft Windows Font Resource Refcount Integer Overflow Privilege Escalation (2709162)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1867

[Update Details](#)

Recommendation is updated

**13777 - (MS12-041) Microsoft Windows String Atom Class Name Handling Privilege Escalation I (2709162)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1864

[Update Details](#)

Recommendation is updated

**13778 - (MS12-041) Microsoft Windows String Atom Class Name Handling Privilege Escalation II (2709162)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1865

[Update Details](#)

Recommendation is updated

**13781 - (MS12-042) Microsoft Windows User Mode Scheduler Memory Corruption Privilege Escalation (2711167)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-0217

[Update Details](#)

Recommendation is updated

**13785 - (MS12-041) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2709162)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1864, CVE-2012-1865, CVE-2012-1866, CVE-2012-1867, CVE-2012-1868

[Update Details](#)

Recommendation is updated

**13859 - (MS12-047) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2718523)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1890, CVE-2012-1893

[Update Details](#)

Recommendation is updated

**13860 - (MS12-047) Microsoft Windows Keyboard Layout Privilege Escalation (2718523)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1890

[Update Details](#)

Recommendation is updated

**13861 - (MS12-047) Microsoft Windows Win32k Incorrect Type Handling Privilege Escalation (2718523)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-1893

[Update Details](#)

Recommendation is updated

**14016 - (MS12-055) Microsoft Windows Win32K User After Free Privilege Escalation (2731847)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2527

[Update Details](#)

Recommendation is updated

**14215 - (MS12-068) Microsoft Windows Integer Overflow Information Disclosure (2724197)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2529

[Update Details](#)

Recommendation is updated

#### **14218 - (MS12-068) Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2724197)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2529

[Update Details](#)

Recommendation is updated

#### **14375 - (MS12-075) Microsoft Windows Win32k Use AfterFree Privilege Escalation I (2761226)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2530

[Update Details](#)

Recommendation is updated

#### **14376 - (MS12-075) Microsoft Windows Win32k Use After Free Privilege Escalation II (2761159)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2553

[Update Details](#)

Recommendation is updated

#### **14562 - (MS13-005) Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0008

[Update Details](#)

Recommendation is updated

#### **14563 - (MS13-005) Microsoft Windows Privilege Escalation (2778930)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0008

[Update Details](#)

Recommendation is updated

---

### 14690 - (MS13-019) Microsoft Windows CSRSS Reference Count Local Privilege Escalation (2790113)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-0076

#### Update Details

Recommendation is updated

### 14716 - (MS13-017) Microsoft Windows Race Condition I Privilege Escalation (2799494)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1278

#### Update Details

Recommendation is updated

### 14717 - (MS13-017) Microsoft Windows Race Condition II Privilege Escalation (2799494)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1279

#### Update Details

Recommendation is updated

### 14718 - (MS13-017) Microsoft Windows Reference Count Privilege Escalation (2799494)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1280

#### Update Details

Recommendation is updated

### 14930 - (MS13-036) Microsoft Windows Kernel OpenType Font Parsing Privilege Escalation (2829996)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1291

#### Update Details

Recommendation is updated

### 15069 - (MS13-046) Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege (2840221)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1332, CVE-2013-1333, CVE-2013-1334

Update Details

Recommendation is updated

**15070 - (MS13-046) Microsoft Windows DirectX Graphics Kernel Subsystem Double Fetch Privilege Escalation (2840221)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1332

Update Details

Recommendation is updated

**15071 - (MS13-046) Microsoft Windows Win32k Buffer Overflow Privilege Escalation (2840221)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1333

Update Details

Recommendation is updated

**15072 - (MS13-046) Microsoft Windows Win32k Window Handle Privilege Escalation (2840221)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1334

Update Details

Recommendation is updated

**15281 - (MS13-053) Microsoft Windows Kernel Read AV Remote Code Execution (2850851)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3660

Update Details

Recommendation is updated

**15365 - (MS13-063) Vulnerabilities In Windows Kernel Could Allow Elevation Of Privilege (2859537)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-2556, CVE-2013-3196, CVE-2013-3197, CVE-2013-3198

Update Details

Recommendation is updated

**15576 - (MS13-076) Vulnerabilities In Kernel-Mode Drivers Could Allow Elevation Of Privilege (2876315)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-1341, CVE-2013-1342, CVE-2013-1343, CVE-2013-1344, CVE-2013-3864, CVE-2013-3865, CVE-2013-3866

Update Details

Recommendation is updated

**16014 - (MS13-096) Microsoft Graphics Component Memory Corruption Remote Code Execution (2908005)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3906

Update Details

Recommendation is updated

**16023 - (MS13-097) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2898785)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-5047

Update Details

Recommendation is updated

**16024 - (MS13-101) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2013-3899, CVE-2013-3902, CVE-2013-3903, CVE-2013-3907, CVE-2013-5058

Update Details

Recommendation is updated

**16207 - (MS14-003) Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2913602)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0262

[Update Details](#)

Recommendation is updated

**16397 - (MS14-014) Vulnerability in Silverlight Could Allow Security Feature Bypass (2932677)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0319

[Update Details](#)

Recommendation is updated

**16398 - (MS14-014) Vulnerability in Silverlight Could Allow Security Feature Bypass (2932677)**

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2014-0319

[Update Details](#)

Recommendation is updated

**16399 - (MS14-014) Microsoft Silverlight DEP/ASLR Security Bypass (2932677)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0319

[Update Details](#)

Recommendation is updated

**16400 - (MS14-015) Vulnerabilities in Windows Kernel Mode Driver Could Allow Elevation of Privilege (2930275)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0300, CVE-2014-0323

[Update Details](#)

Recommendation is updated

**16401 - (MS14-015) Microsoft Windows Kernel Mode Driver Win32k Privilege Escalation Privilege (2930275)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0300

[Update Details](#)

Recommendation is updated

#### **16964 - (MS14-047) Vulnerability in LRPC Could Allow Security Feature Bypass (2978668)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0316

[Update Details](#)

Recommendation is updated

#### **16965 - (MS14-047) Microsoft Windows ASLR Bypass Security Bypass (2978668)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-0316

[Update Details](#)

Recommendation is updated

#### **17408 - (MS14-079) Vulnerability in Kernel-Mode Driver Could Allow Denial of Service (3002885)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6317

[Update Details](#)

Recommendation is updated

#### **17409 - (MS14-079) Microsoft Windows Kernel Denial of Service (3002885)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2014-6317

[Update Details](#)

Recommendation is updated

#### **17592 - (MS15-001) Vulnerability in Windows AppCompatCache could allow Elevation of Privilege (3023266)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0002

[Update Details](#)

Recommendation is updated

---



### 17593 - (MS15-001) Microsoft Windows Application Compatibility Infrastructure Privilege Escalation (3023266)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0002

#### Update Details

Recommendation is updated

### 17816 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXII Remote Code Execution (3034682)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0042

#### Update Details

Recommendation is updated

### 17817 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXIII Remote Code Execution (3034682)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0043

#### Update Details

Recommendation is updated

### 17850 - (MS15-010) Microsoft Windows Win32k Privilege Escalation I (3036220)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0003

#### Update Details

Recommendation is updated

### 17851 - (MS15-010) Microsoft Windows CNG Feature Security Bypass (3036220)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0010

#### Update Details

Recommendation is updated

### 17852 - (MS15-010) Microsoft Windows Win32k Privilege Escalation II (3036220)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0057

Update Details

Recommendation is updated

**17853 - (MS15-010) Microsoft Windows Cursor Object Double Free Privilege Escalation (3036220)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0058

Update Details

Recommendation is updated

**17855 - (MS15-010) Microsoft Windows Font Driver Denial of Service (3036220)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0060

Update Details

Recommendation is updated

**17857 - (MS15-010) Vulnerabilities in Windows Kernel Mode Driver Could Allow Remote Code Execution (3036220)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0003, CVE-2015-0010, CVE-2015-0057, CVE-2015-0058, CVE-2015-0059, CVE-2015-0060

Update Details

Recommendation is updated

**18024 - (MS15-023) Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege (3034344)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0077, CVE-2015-0078, CVE-2015-0094, CVE-2015-0095

Update Details

Recommendation is updated

**18029 - (MS15-025) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (3038680)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-0073, CVE-2015-0075

Update Details

Recommendation is updated

**18151 - (MS15-038) Microsoft Windows NtCreateTransactionManager Type Confusion Privilege Escalation (3049576)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1643

Update Details

Recommendation is updated

**18170 - (MS15-038) Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (3049576)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1643, CVE-2015-1644

Update Details

Recommendation is updated

**18462 - (MS15-061) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057839)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1719, CVE-2015-1720, CVE-2015-1721, CVE-2015-1722, CVE-2015-1723, CVE-2015-1724, CVE-2015-1725, CVE-2015-1726, CVE-2015-1727, CVE-2015-1768, CVE-2015-2360

Update Details

Recommendation is updated

**18464 - (MS15-061) Microsoft Windows Kernel Use-After-Free Privilege Escalation (3057839)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1720

Update Details

Recommendation is updated

**18465 - (MS15-061) Microsoft Windows Win32k Null Pointer Dereference Privilege Escalation (3057839)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1721

[Update Details](#)

Recommendation is updated

**18467 - (MS15-061) Microsoft Windows Kernel Bitmap Handling Use-After-Free Privilege Escalation (3057839)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1722

[Update Details](#)

Recommendation is updated

**18468 - (MS15-061) Microsoft Windows Station Use-After-Free Privilege Escalation (3057839)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1723

[Update Details](#)

Recommendation is updated

**18470 - (MS15-061) Microsoft Windows Win32k Buffer Overflow Privilege Escalation (3057839)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1725

[Update Details](#)

Recommendation is updated

**18474 - (MS15-061) Microsoft Windows Win32k Privilege Escalation (3057839)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2360

[Update Details](#)

Recommendation is updated

**18589 - (MS15-073) Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (3070102)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2363, CVE-2015-2365, CVE-2015-2366, CVE-2015-2367, CVE-2015-2381, CVE-2015-2382

[Update Details](#)

Recommendation is updated

**18597 - (MS15-073) Microsoft Windows Kernel I Privilege Escalation (3070102)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2363

[Update Details](#)

Recommendation is updated

**18598 - (MS15-073) Microsoft Windows Kernel II Privilege Escalation (3070102)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2365

[Update Details](#)

Recommendation is updated

**18599 - (MS15-073) Microsoft Windows Kernel III Privilege Escalation (3070102)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2366

[Update Details](#)

Recommendation is updated

**18603 - (MS15-076) Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege (3067505)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2370

[Update Details](#)

Recommendation is updated

**18604 - (MS15-076) Microsoft Windows DCOM RPC Privilege Escalation (3067505)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2370

[Update Details](#)

Recommendation is updated

### 18799 - (MS15-085) Microsoft Windows Mount Manager Privilege Escalation (3082487)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1769

#### Update Details

Recommendation is updated

### 18806 - (MS15-085) Vulnerability in Mount Manager Could Allow Elevation of Privilege (3082487)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-1769

#### Update Details

Recommendation is updated

### 18952 - (MS15-102) Microsoft Windows Task Scheduler III Privilege Escalation (3089657)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2528

#### Update Details

Recommendation is updated

### 18953 - (MS15-102) Microsoft Windows Task Scheduler II Privilege Escalation (3089657)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2525

#### Update Details

Recommendation is updated

### 18954 - (MS15-102) Microsoft Windows Task Scheduler Privilege Escalation (3089657)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2524

#### Update Details

Recommendation is updated

### 18955 - (MS15-102) Vulnerability in Windows Task Management Could Allow Elevation of Privilege (3089657)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2524, CVE-2015-2525, CVE-2015-2528

#### Update Details

Recommendation is updated

### 18961 - (MS15-097) Microsoft Windows Graphics Font Driver I Privilege Escalation (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2507

#### Update Details

Recommendation is updated

### 18962 - (MS15-097) Microsoft Windows Graphics Font Driver II Privilege Escalation (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2508

#### Update Details

Recommendation is updated

### 18964 - (MS15-097) Microsoft Windows Graphics Memory Corruption I Remote Code Execution (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2511

#### Update Details

Recommendation is updated

### 18965 - (MS15-097) Microsoft Windows Graphics Memory Corruption II Privilege Escalation (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2512

#### Update Details

Recommendation is updated

### 18966 - (MS15-097) Microsoft Windows Graphics Memory Corruption III Privilege Escalation (3089656)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2517

Update Details

Recommendation is updated

**18967 - (MS15-097) Microsoft Windows Graphics Privilege Escalation (3089656)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2518

Update Details

Recommendation is updated

**18968 - (MS15-097) Microsoft Windows Graphics ASLR Privilege Escalation (3089656)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2527

Update Details

Recommendation is updated

**18972 - (MS15-097) Microsoft Windows Graphics Memory Corruption IV Privilege Escalation (3089656)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2546

Update Details

Recommendation is updated

**19098 - (MS15-111) Microsoft Windows Kernel Memory Corruption Privilege Escalation (3096447)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-2549

Update Details

Recommendation is updated

**19099 - (MS15-111) Microsoft Windows Elevation Privilege Escalation (3096447)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)



Risk Level: High  
CVE: CVE-2015-2550

Update Details

Recommendation is updated

**19101 - (MS15-111) Microsoft Windows Mount Point Privilege Escalation (3096447)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2015-2553

Update Details

Recommendation is updated

**19102 - (MS15-111) Microsoft Windows Object Privilege Escalation (3096447)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2015-2554

Update Details

Recommendation is updated

**19104 - (MS15-111) Security Update for Windows Kernel to Address Elevation of Privilege (3096447)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2015-2549, CVE-2015-2550, CVE-2015-2552, CVE-2015-2553, CVE-2015-2554

Update Details

Recommendation is updated

**19215 - (MS15-119) Microsoft Windows Winsock Valid Memory Address Privilege Escalation (3104521)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2015-2478

Update Details

Recommendation is updated

**19217 - (MS15-119) Security Update in Winsock to Address Elevation of Privilege (3104521)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2015-2478

[Update Details](#)

Recommendation is updated

**19224 - (MS15-115) Microsoft Windows Kernel Privilege Escalation I (3105864)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6100

[Update Details](#)

Recommendation is updated

**19225 - (MS15-115) Microsoft Windows Kernel Privilege Escalation II (3105864)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6101

[Update Details](#)

Recommendation is updated

**19348 - (MS15-133) Security Update for Windows PGM to Address Elevation of Privilege (3116130)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6126

[Update Details](#)

Recommendation is updated

**19349 - (MS15-133) Microsoft Windows PGM UAF Privilege Escalation (3116130)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6126

[Update Details](#)

Recommendation is updated

**19389 - (MS15-132) Microsoft Windows Library Loading Privilege Escalation I (3116162)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6128

[Update Details](#)

Recommendation is updated

### **19391 - (MS15-132) Microsoft Windows Library Loading Privilege Escalation III (3116162)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6132

[Update Details](#)

Recommendation is updated

### **19392 - (MS15-132) Microsoft Windows Library Loading Privilege Escalation IV (3116162)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6133

[Update Details](#)

Recommendation is updated

### **19393 - (MS15-135) Microsoft Windows Kernel Memory Privilege Escalation I (3119075)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6171

[Update Details](#)

Recommendation is updated

### **19394 - (MS15-135) Microsoft Windows Kernel Memory Privilege Escalation II (3119075)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6173

[Update Details](#)

Recommendation is updated

### **19395 - (MS15-135) Microsoft Windows Kernel Memory Privilege Escalation III (3119075)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6174

[Update Details](#)

Recommendation is updated

### 19396 - (MS15-135) Microsoft Windows Kernel Memory Privilege Escalation IV (3119075)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6175

#### Update Details

Recommendation is updated

### 19400 - (MS15-132) Security Update for Microsoft Windows to Address Remote Code Execution (3116162)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6128, CVE-2015-6132, CVE-2015-6133

#### Update Details

Recommendation is updated

### 19401 - (MS15-135) Security Update for Windows Kernel Mode Drivers to Address Elevation of Privilege (3119075)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2015-6171, CVE-2015-6173, CVE-2015-6174, CVE-2015-6175

#### Update Details

Recommendation is updated

### 19646 - (MS16-018) Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3136082)

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0048

#### Update Details

Recommendation is updated

### 19648 - (MS16-018) Microsoft Windows Win32k Privilege Escalation (3136082)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0048

#### Update Details

Recommendation is updated

### 19656 - (MS16-017) Microsoft Remote Desktop Protocol Privilege Escalation (3134700)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0036

Update Details

Recommendation is updated

**19657 - (MS16-017) Security Update for Remote Desktop Display Driver to Address Elevation of Privilege (3134700)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0036

Update Details

Recommendation is updated

**19658 - (MS16-016) Microsoft Windows WebDAV Privilege Escalation (3136041)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0051

Update Details

Recommendation is updated

**19659 - (MS16-016) Security Update for WebDAV to Address Elevation of Privilege (3136041)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0051

Update Details

Recommendation is updated

**19664 - (MS16-014) Microsoft Windows Elevation Privilege Escalation (3134228)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0040

Update Details

Recommendation is updated

**19665 - (MS16-014) Microsoft Windows DLL Loading Remote Code Execution (3134228)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-0041

Update Details

Recommendation is updated

**19666 - (MS16-014) Microsoft Windows DLL Loading Remote Code Execution II (3134228)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-0042

Update Details

Recommendation is updated

**19673 - (MS16-014) Security Update for Microsoft Windows to Address Remote Code Execution (3134228)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-0040, CVE-2016-0041, CVE-2016-0042, CVE-2016-0044, CVE-2016-0049

Update Details

Recommendation is updated

**19682 - (MS16-011) Microsoft Edge Memory Corruption Remote Code Execution III (3134225)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-0060

Update Details

Recommendation is updated

**19747 - (MS16-024) Cumulative Security Update for Microsoft Edge (3142019)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-0102, CVE-2016-0105, CVE-2016-0109, CVE-2016-0110, CVE-2016-0111, CVE-2016-0116, CVE-2016-0123, CVE-2016-0124, CVE-2016-0125, CVE-2016-0129, CVE-2016-0130

Update Details

Recommendation is updated

**19763 - (MS16-034) Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3143145)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0093, CVE-2016-0094, CVE-2016-0095, CVE-2016-0096

Update Details

Recommendation is updated

**19770 - (MS16-023) Cumulative Security Update for Internet Explorer (3142015)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0102, CVE-2016-0103, CVE-2016-0104, CVE-2016-0105, CVE-2016-0106, CVE-2016-0107, CVE-2016-0108, CVE-2016-0109, CVE-2016-0110, CVE-2016-0111, CVE-2016-0112, CVE-2016-0113, CVE-2016-0114

Update Details

Recommendation is updated

**19790 - (MS16-026) Microsoft Windows Adobe Type Manager Library OpenFont Parsing Denial of Service (3143148)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0120

Update Details

Recommendation is updated

**19904 - (MS16-038) Cumulative Security Update for Microsoft Edge (3148532)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0154, CVE-2016-0155, CVE-2016-0156, CVE-2016-0157, CVE-2016-0158, CVE-2016-0161

Update Details

Recommendation is updated

**19906 - (MS16-048) Microsoft Windows CSRSS Security Bypass (3148528)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0151

Update Details

Recommendation is updated

**19922 - (MS16-045) Security Update for Windows Hyper-V (3143118)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0088, CVE-2016-0089, CVE-2016-0090

[Update Details](#)

Recommendation is updated

**19937 - (MS16-037) Cumulative Security Update for Internet Explorer (3148531)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0154, CVE-2016-0159, CVE-2016-0160, CVE-2016-0162, CVE-2016-0164, CVE-2016-0166

[Update Details](#)

Recommendation is updated

**20011 - (MS16-051) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution I (3155533)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0187

[Update Details](#)

Recommendation is updated

**20013 - (MS16-051) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution (3155533)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0189

[Update Details](#)

Recommendation is updated

**20014 - (MS16-051) Microsoft Internet Explorer Browser Memory Corruption Remote Code Execution (3155533)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0192

[Update Details](#)

Recommendation is updated

**20026 - (MS16-052) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution I (3155538)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0186

[Update Details](#)



Recommendation is updated

#### **20027 - (MS16-052) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution II (3155538)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0191

[Update Details](#)

Recommendation is updated

#### **20028 - (MS16-052) Microsoft Edge Scripting Engine Memory Corruption Remote Code Execution III (3155538)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0193

[Update Details](#)

Recommendation is updated

#### **20029 - (MS16-052) Microsoft Edge Memory Corruption Remote Code Execution (3155538)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0192

[Update Details](#)

Recommendation is updated

#### **20036 - (MS16-062) Microsoft Windows Kernel DirectX Subsystem Privilege Escalation I (3158222)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0176

[Update Details](#)

Recommendation is updated

#### **20038 - (MS16-062) Microsoft Windows Kernel Privilege Escalation IV (3158222)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0174

[Update Details](#)

Recommendation is updated

---

### **20039 - (MS16-062) Microsoft Windows Kernel Privilege Escalation III (3158222)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0173

#### Update Details

Recommendation is updated

### **20041 - (MS16-062) Microsoft Windows Kernel Privilege Escalation I (3158222)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0171

#### Update Details

Recommendation is updated

### **20042 - (MS16-062) Security Update for Windows Kernel-Mode Drivers (3158222)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0171, CVE-2016-0173, CVE-2016-0174, CVE-2016-0175, CVE-2016-0176, CVE-2016-0196, CVE-2016-0197

#### Update Details

Recommendation is updated

### **20043 - (MS16-060) Microsoft Windows Kernel Symbolic Links Privilege Escalation (3154846)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0180

#### Update Details

Recommendation is updated

### **20045 - (MS16-062) Microsoft Windows Kernel DirectX Subsystem Privilege Escalation II (3158222)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0197

#### Update Details

Recommendation is updated

### **20048 - (MS16-060) Security Update for Windows Kernel (3154846)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0180

Update Details

Recommendation is updated

**20050 - (MS16-062) Microsoft Windows Kernel Privilege Escalation V (3158222)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0196

Update Details

Recommendation is updated

**20064 - (MS16-052) Cumulative Security Update for Microsoft Edge (3155538)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-0186, CVE-2016-0191, CVE-2016-0192, CVE-2016-0193

Update Details

Recommendation is updated

**20152 - (MS16-068) Microsoft Edge Chakra Scripting Engine Memory Corruption Remote Code Execution II (3163656)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3202

Update Details

Recommendation is updated

**20155 - (MS16-068) Microsoft Edge Memory Corruption Remote Code Execution (3163656)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3222

Update Details

Recommendation is updated

**20165 - (MS16-063) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3163649)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-0200

Update Details

Recommendation is updated

**20166 - (MS16-063) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution I (3163649)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-3202

Update Details

Recommendation is updated

**20167 - (MS16-063) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution II (3163649)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-3205

Update Details

Recommendation is updated

**20168 - (MS16-063) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution III (3163649)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-3206

Update Details

Recommendation is updated

**20169 - (MS16-063) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution IV (3163649)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-3207

Update Details

Recommendation is updated

**20170 - (MS16-063) Microsoft Internet Explorer Scripting Engine Memory Corruption Remote Code Execution V (3163649)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High  
CVE: CVE-2016-3210

[Update Details](#)

Recommendation is updated

**20171 - (MS16-063) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3163649)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3211

[Update Details](#)

Recommendation is updated

**20172 - (MS16-063) Microsoft Internet Explorer XSS Filter Javascript Validation Remote Code Execution (3163649)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3212

[Update Details](#)

Recommendation is updated

**20255 - (MS16-090) Security Update for Windows Kernel-Mode Drivers (3171481)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3249, CVE-2016-3250, CVE-2016-3251, CVE-2016-3252, CVE-2016-3254, CVE-2016-3286

[Update Details](#)

Recommendation is updated

**20266 - (MS16-090) Microsoft Windows Kernel Privilege Escalation (3171481)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3286

[Update Details](#)

Recommendation is updated

**20267 - (MS16-090) Microsoft Windows Kernel Privilege Escalation IV (3171481)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3254

[Update Details](#)

Recommendation is updated

#### **20268 - (MS16-090) Microsoft Windows Kernel Privilege Escalation III (3171481)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3252

[Update Details](#)

Recommendation is updated

#### **20270 - (MS16-090) Microsoft Windows Kernel Privilege Escalation II (3171481)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3250

[Update Details](#)

Recommendation is updated

#### **20271 - (MS16-090) Microsoft Windows Kernel Privilege Escalation I (3171481)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3249

[Update Details](#)

Recommendation is updated

#### **20274 - (MS16-087) Microsoft Windows Print Spooler File System Writing Privilege Escalation (3170005)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3239

[Update Details](#)

Recommendation is updated

#### **20291 - (MS16-084) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3243

[Update Details](#)

Recommendation is updated

### **20292 - (MS16-084) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3242

#### Update Details

Recommendation is updated

### **20293 - (MS16-084) Microsoft Internet Explorer Memory Corruption Remote Code Execution II (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3241

#### Update Details

Recommendation is updated

### **20294 - (MS16-084) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3240

#### Update Details

Recommendation is updated

### **20309 - (MS16-085) Microsoft Edge Memory Corruption Remote Code Execution I (3169999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3246

#### Update Details

Recommendation is updated

### **20385 - (MS16-102) Security Update for Microsoft Windows PDF Library (3182248)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3319

#### Update Details

Recommendation is updated

### **20389 - (MS16-096) Microsoft Edge PDF Remote Code Execution (3177358)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3319

Update Details

Recommendation is updated

**20398 - (MS16-101) Security Update for Windows Authentication Methods (3178465)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3237, CVE-2016-3300

Update Details

Recommendation is updated

**20412 - (MS16-095) Cumulative Security Update for Internet Explorer (3177356)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3288, CVE-2016-3289, CVE-2016-3290, CVE-2016-3293, CVE-2016-3321, CVE-2016-3322, CVE-2016-3326, CVE-2016-3327, CVE-2016-3329

Update Details

Recommendation is updated

**20416 - (MS16-098) Security Update for Windows Kernel-Mode Drivers (3178466)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3308, CVE-2016-3309, CVE-2016-3310, CVE-2016-3311

Update Details

Recommendation is updated

**20503 - (MS16-105) Cumulative Security Update for Microsoft Edge (3183043)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3247, CVE-2016-3291, CVE-2016-3294, CVE-2016-3295, CVE-2016-3297, CVE-2016-3325, CVE-2016-3330, CVE-2016-3350, CVE-2016-3351, CVE-2016-3370, CVE-2016-3374, CVE-2016-3377

Update Details

Recommendation is updated

**20533 - (MS16-104) Cumulative Security Update for Internet Explorer (3183038)**



Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3247, CVE-2016-3291, CVE-2016-3292, CVE-2016-3295, CVE-2016-3297, CVE-2016-3324, CVE-2016-3325, CVE-2016-3351, CVE-2016-3353, CVE-2016-3375

Update Details

Recommendation is updated

**20534 - (MS16-104) Microsoft Internet Explorer Memory Corruption Remote Code Execution I (3183038)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-3247

Update Details

Recommendation is updated

**88807 - Slackware Linux 13.0, 13.1, 13.37, 14.0, 14.1, 14.2 SSA:2016-259-01 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Slackware Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-7167

Update Details

Risk is updated

**182119 - FreeBSD cURL Escape And Unescape Integer Overflows (b018121b-7a4b-11e6-bf52-b499baebfeaf)**

Category: SSH Module -> NonIntrusive -> FreeBSD Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-7167

Update Details

Risk is updated

**190726 - Fedora Linux 24 FEDORA-2016-e84b809c4b Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-1000003

Update Details

Risk is updated

**190920 - Fedora Linux 22 FEDORA-2016-b2ad500fea Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-1000003

[Update Details](#)

Risk is updated

#### 190921 - Fedora Linux 23 FEDORA-2016-7a1853cd7d Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-1000003

[Update Details](#)

Risk is updated

#### 191123 - Fedora Linux 25 FEDORA-2016-08533fc59c Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-7167

[Update Details](#)

Risk is updated

#### 191130 - Fedora Linux 24 FEDORA-2016-7a2ed52d41 Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-7167

[Update Details](#)

Risk is updated

#### 191192 - Fedora Linux 23 FEDORA-2016-80f4f71eff Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: High

CVE: CVE-2016-7167

[Update Details](#)

Risk is updated

#### 6164 - (MS08-064) Microsoft Virtual Address Descriptor Elevation of Privilege Vulnerability (956841)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-4036

[Update Details](#)

Recommendation is updated

#### 6169 - (MS08-061) Microsoft Windows Kernel Window Creation Vulnerability (954211)

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-2250

Update Details

Recommendation is updated

**6170 - (MS08-061) Microsoft Windows Kernel Unhandled Exception Vulnerability (954211)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-2251

Update Details

Recommendation is updated

**6171 - (MS08-061) Microsoft Windows Kernel Memory Corruption Vulnerability (954211)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-2252

Update Details

Recommendation is updated

**6493 - (MS09-006) Windows Kernel Handle Validation Vulnerability (958690)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0082

Update Details

Recommendation is updated

**6494 - (MS09-006) Windows Kernel Invalid Pointer Vulnerability (958690)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-0083

Update Details

Recommendation is updated

**6766 - (MS09-025) Microsoft Windows Desktop Parameter Edit Vulnerability (968537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2009-1126

[Update Details](#)

Recommendation is updated

**6767 - (MS09-025) Microsoft Windows Driver Class Registration Vulnerability (968537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2009-1125

[Update Details](#)

Recommendation is updated

**6768 - (MS09-025) Microsoft Windows Kernel Desktop Vulnerability (968537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2009-1123

[Update Details](#)

Recommendation is updated

**6769 - (MS09-025) Microsoft Windows Kernel Pointer Validation Vulnerability (968537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2009-1124

[Update Details](#)

Recommendation is updated

**7203 - (MS09-058) Windows Kernel Integer Underflow Vulnerability (971486)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2009-2515

[Update Details](#)

Recommendation is updated

**7204 - (MS09-058) Windows Kernel NULL Pointer Dereference Vulnerability (971486)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2009-2516

[Update Details](#)

Recommendation is updated

**7342 - Microsoft Windows SMB\_PACKET Remote Kernel Denial-of-Service Vulnerability**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-3676

[Update Details](#)

Recommendation is updated

**7544 - (MS09-025) Vulnerabilities In Windows Kernel Could Allow Elevation of Privilege (968537)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-1123, CVE-2009-1124, CVE-2009-1125, CVE-2009-1126

[Update Details](#)

Recommendation is updated

**8054 - (MS08-064) Vulnerability In Virtual Address Descriptor Manipulation Could Allow Elevation Of Privilege (956841)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2008-4036

[Update Details](#)

Recommendation is updated

**8521 - (MS10-021) Microsoft Windows Kernel Memory Allocation Vulnerability (979683)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0236

[Update Details](#)

Recommendation is updated

**8522 - (MS10-021) Microsoft Windows Kernel Symbolic Link Creation Vulnerability (979683)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0237

[Update Details](#)

Recommendation is updated

#### **9073 - (MS10-032) Microsoft Windows Win32k Improper Data Validation Vulnerability (979559)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0484

[Update Details](#)

Recommendation is updated

#### **9074 - (MS10-032) Microsoft Windows Win32k Window Creation Vulnerability (979559)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0485

[Update Details](#)

Recommendation is updated

#### **9075 - (MS10-032) Microsoft Windows Win32k TrueType Font Parsing Vulnerability (979559)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1255

[Update Details](#)

Recommendation is updated

#### **9682 - (MS10-047) Microsoft Windows Kernel Improper Validation Denial Of Service (981852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1890

[Update Details](#)

Recommendation is updated

#### **9683 - (MS10-047) Microsoft Windows Kernel Double Free Privilege Escalation (981852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1889

[Update Details](#)

Recommendation is updated

### **9684 - (MS10-047) Microsoft Windows Kernel Data Initialization Privilege Escalation (981852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1888

#### Update Details

Recommendation is updated

### **10358 - (MS10-073) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2549, CVE-2010-2743, CVE-2010-2744

#### Update Details

Recommendation is updated

### **10360 - (MS10-073) Microsoft Windows Win32K Reference Count Privilege Escalation (981957)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2549

#### Update Details

Recommendation is updated

### **10361 - (MS10-073) Microsoft Windows Win32K Keyboard Layout Privilege Escalation (981957)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2743

#### Update Details

Recommendation is updated

### **10362 - (MS10-073) Microsoft Windows Win32k Window Class Privilege Escalation (981957)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-2744

#### Update Details

Recommendation is updated

### **16046 - (MS13-100) Vulnerabilities in Microsoft SharePoint Server Could Allow Elevation of Privilege (2904244)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5059

[Update Details](#)

Recommendation is updated

**16402 - (MS14-015) Microsoft Windows Kernel Mode Driver Win32k Information Disclosure (2930275)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0323

[Update Details](#)

Recommendation is updated

**16496 - (MS14-019) Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2922229)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0315

[Update Details](#)

Recommendation is updated

**16745 - (MS14-035) Microsoft Internet Explorer Privilege Escalation II (2969262)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1778

[Update Details](#)

Recommendation is updated

**16759 - (MS14-035) Microsoft Internet Explorer TLS Server Certificate Renegotiation Information Disclosure (2969262)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1771

[Update Details](#)

Recommendation is updated

**16845 - (MS14-037) Microsoft Internet Explorer Extended Validation Certificate Security Bypass (2975687)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)



Risk Level: Medium  
CVE: CVE-2014-2783

[Update Details](#)

Recommendation is updated

**16969 - (MS14-051) Microsoft Internet Explorer Privilege Escalation II (2976627)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2014-2819

[Update Details](#)

Recommendation is updated

**16970 - (MS14-051) Microsoft Internet Explorer Privilege Escalation I (2976627)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2014-2817

[Update Details](#)

Recommendation is updated

**17232 - (MS14-056) Microsoft Internet Explorer I Privilege Escalation (2987107)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2014-4123

[Update Details](#)

Recommendation is updated

**17233 - (MS14-056) Microsoft Internet Explorer II Privilege Escalation (2987107)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2014-4124

[Update Details](#)

Recommendation is updated

**17234 - (MS14-056) Microsoft Internet Explorer ASLR Security Bypass (2987107)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2014-4140

[Update Details](#)

Recommendation is updated

**17835 - (MS15-009) Microsoft Internet Explorer Memory Corruption XXXV Remote Code Execution (3034682)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-8967

[Update Details](#)

Recommendation is updated

**17837 - (MS15-009) Cumulative Security Update for Internet Explorer (3034682)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-8967, CVE-2015-0017, CVE-2015-0018, CVE-2015-0019, CVE-2015-0020, CVE-2015-0021, CVE-2015-0022, CVE-2015-0023, CVE-2015-0025, CVE-2015-0026, CVE-2015-0027, CVE-2015-0028, CVE-2015-0029, CVE-2015-0030, CVE-2015-0031, CVE-2015-0035, CVE-2015-0036, CVE-2015-0037, CVE-2015-0038, CVE-2015-0039, CVE-2015-0040, CVE-2015-0041, CVE-2015-0042, CVE-2015-0043, CVE-2015-0044, CVE-2015-0045, CVE-2015-0046, CVE-2015-0048, CVE-2015-0049, CVE-2015-0050, CVE-2015-0051, CVE-2015-0052, CVE-2015-0053, CVE-2015-0054, CVE-2015-0055, CVE-2015-0066, CVE-2015-0067, CVE-2015-0068, CVE-2015-0069, CVE-2015-0070, CVE-2015-0071

[Update Details](#)

Recommendation is updated

**18287 - (MS15-043) Microsoft Internet Explorer Privilege Escalation I (3049563)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1688

[Update Details](#)

Recommendation is updated

**18293 - (MS15-043) Microsoft Internet Explorer Privilege Escalation II (3049563)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1703

[Update Details](#)

Recommendation is updated

**18294 - (MS15-043) Microsoft Internet Explorer Privilege Escalation III (3049563)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-1704

[Update Details](#)

Recommendation is updated

**18303 - (MS15-043) Microsoft Internet Explorer Privilege Escalation IV (3049563)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-1713

[Update Details](#)

Recommendation is updated

**18435 - (MS15-056) Microsoft Internet Explorer Permissions III Privilege Escalation (3058515)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-1748

[Update Details](#)

Recommendation is updated

**18439 - (MS15-056) Microsoft Internet Explorer Permissions II Privilege Escalation (3058515)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-1743

[Update Details](#)

Recommendation is updated

**18443 - (MS15-056) Microsoft Internet Explorer Permissions I Privilege Escalation (3058515)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-1739

[Update Details](#)

Recommendation is updated

**18461 - (MS15-063) Microsoft Windows LoadLibrary Privilege Escalation (3063858)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1758

[Update Details](#)

Recommendation is updated

**18477 - (MS15-063) Vulnerability in Windows Kernel Could Allow Elevation of Privilege (3063858)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1758

[Update Details](#)

Recommendation is updated

**18610 - (MS15-070) Microsoft Excel DLL Remote Code Execution (3072620)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2378

[Update Details](#)

Recommendation is updated

**18931 - (MS15-094) Microsoft Internet Explorer File Flags Tampering Privilege Escalation (3089548)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2484

[Update Details](#)

Recommendation is updated

**19084 - (MS15-106) Microsoft Internet Explorer I Privilege Escalation (3096441)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6044

[Update Details](#)

Recommendation is updated

**19088 - (MS15-106) Microsoft Internet Explorer II Privilege Escalation (3096441)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6047

[Update Details](#)

Recommendation is updated

**19100 - (MS15-111) Microsoft Windows Trusted Boot Security Bypass (3096447)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2552

[Update Details](#)

Recommendation is updated

**19513 - (MS16-007) Security Update for Microsoft Windows to Address Remote Code Execution (3124901)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0014, CVE-2016-0015, CVE-2016-0016, CVE-2016-0018, CVE-2016-0019, CVE-2016-0020

[Update Details](#)

Recommendation is updated

**19544 - (MS16-008) Security Update for Windows Kernel to Address Elevation of Privilege (3124605)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0006, CVE-2016-0007

[Update Details](#)

Recommendation is updated

**20184 - (MS16-078) Security Update for Windows Diagnostic Hub (3165479)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3231

[Update Details](#)

Recommendation is updated

**7202 - (MS09-058) Windows Kernel Exception Handler Vulnerability (971486)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-2517

[Update Details](#)

Recommendation is updated

### **8519 - (MS10-021) Microsoft Windows Kernel Null Pointer Vulnerability (979683)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0234

#### Update Details

Recommendation is updated

### **8520 - (MS10-021) Microsoft Windows Kernel Symbolic Link Value Vulnerability (979683)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0235

#### Update Details

Recommendation is updated

### **8523 - (MS10-021) Microsoft Windows Kernel Registry Key Vulnerability (979683)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0238

#### Update Details

Recommendation is updated

### **8524 - (MS10-021) Microsoft Windows Virtual Path Parsing Vulnerability (979683)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0481

#### Update Details

Recommendation is updated

### **8525 - (MS10-021) Microsoft Windows Kernel Malformed Image Vulnerability (979683)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0482

#### Update Details

Recommendation is updated

### **8526 - (MS10-021) Microsoft Windows Kernel Exception Handler Vulnerability (979683)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0810

#### Update Details

Recommendation is updated

### **9063 - (MS10-032) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Remote Code Execution (979559)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-0484, CVE-2010-0485, CVE-2010-1255

#### Update Details

Recommendation is updated

### **9763 - (MS10-049) Microsoft Windows TLS/SSL Renegotiation Vulnerability (980436)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2009-3555

#### Update Details

Recommendation is updated

### **11175 - (MS11-026) Microsoft MHTML Mime-Formatted Request (2503658)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0096

#### Update Details

Recommendation is updated

### **11225 - (MS11-013) Microsoft Kerberos Spoofing (2496930)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0091

#### Update Details

Recommendation is updated

### **11762 - (MS11-026) Vulnerability in MHTML Could Allow Information Disclosure (2503658)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0096

Update Details

Recommendation is updated

**11770 - (MS11-034) Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2506223)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0662, CVE-2011-0665, CVE-2011-0666, CVE-2011-0667, CVE-2011-0670, CVE-2011-0671, CVE-2011-0672, CVE-2011-0673, CVE-2011-0674, CVE-2011-0676, CVE-2011-0677, CVE-2011-1225, CVE-2011-1226, CVE-2011-1227, CVE-2011-1228, CVE-2011-1229, CVE-2011-1230, CVE-2011-1231, CVE-2011-1232, CVE-2011-1233, CVE-2011-1234, CVE-2011-1235, CVE-2011-1236, CVE-2011-1237, CVE-2011-1238, CVE-2011-1239, CVE-2011-1240, CVE-2011-1241, CVE-2011-1242

Update Details

Recommendation is updated

**12252 - (MS11-037) Vulnerability In MHTML Could Allow Information Disclosure (2544893)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1894

Update Details

Recommendation is updated

**12472 - (MS11-068) Microsoft Kernel Metadata Parsing Could Allow Denial of Service (2556532)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1971

Update Details

Recommendation is updated

**12475 - (MS11-068) Vulnerability in Windows Kernel Could Allow Denial of Service (2556532)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1971

Update Details

Recommendation is updated

**12628 - (MS11-074) Microsoft XSS in SharePoint Calendar Elevation of Privilege (2451858)**



---

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0653

[Update Details](#)

Recommendation is updated

#### **12629 - (MS11-074) Microsoft SharePoint HTML Sanitization Information Disclosure (2451858)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1252

[Update Details](#)

Recommendation is updated

#### **12630 - (MS11-074) Microsoft SharePoint Editform Script Injection Elevation of Privilege (2451858)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1890

[Update Details](#)

Recommendation is updated

#### **12631 - (MS11-074) Microsoft SharePoint Contact Details Reflected XSS Elevation of Privilege (2451858)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1891

[Update Details](#)

Recommendation is updated

#### **12632 - (MS11-074) Microsoft SharePoint Remote File Disclosure Information Disclosure (2451858)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1892

[Update Details](#)

Recommendation is updated

#### **12633 - (MS11-074) Microsoft SharePoint XSS Elevation of Privilege (2451858)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1893

[Update Details](#)

Recommendation is updated

### **12634 - (MS11-074) Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858)**

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-0653, CVE-2011-1252, CVE-2011-1890, CVE-2011-1891, CVE-2011-1892, CVE-2011-1893

[Update Details](#)

Recommendation is updated

### **12739 - (MS11-077) Microsoft Windows Kernel-Mode Drivers Win32k TrueType Font Type Translation (2567053)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-2002

[Update Details](#)

Recommendation is updated

### **13623 - (MS12-034) Microsoft Windows .NET Index Comparison Remote Code Execution (2681578)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0164

[Update Details](#)

Recommendation is updated

### **13779 - (MS12-041) Microsoft Windows Win32k.sys Race Condition Privilege Escalation (2709162)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1868

[Update Details](#)

Recommendation is updated

### **13783 - (MS12-039) Microsoft Windows HTML Sanitization Information Disclosure (2707956)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1858

[Update Details](#)

Recommendation is updated

**13864 - (MS12-050) Microsoft SharePoint HTML Sanitization Information Disclosure (2695502)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1858

[Update Details](#)

Recommendation is updated

**13865 - (MS12-050) Microsoft SharePoint Scriptresx.ashx Cross Site Scripting Privilege Escalation (2695502)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1859

[Update Details](#)

Recommendation is updated

**13866 - (MS12-050) Microsoft SharePoint Search Scope Information Disclosure (2695502)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1860

[Update Details](#)

Recommendation is updated

**13867 - (MS12-050) Microsoft SharePoint Script In Username Privilege Escalation (2695502)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1861

[Update Details](#)

Recommendation is updated

**13868 - (MS12-050) Microsoft SharePoint URL Redirection Information Disclosure (2695502)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1862

[Update Details](#)

Recommendation is updated

**13869 - (MS12-050) Microsoft SharePoint Reflected List Parameter Privilege Escalation (2695502)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1863

[Update Details](#)

Recommendation is updated

**13870 - (MS12-050) Vulnerabilities In Microsoft SharePoint Could Allow Elevation Of Privilege (2695502)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1858, CVE-2012-1859, CVE-2012-1860, CVE-2012-1861, CVE-2012-1862, CVE-2012-1863

[Update Details](#)

Recommendation is updated

**13874 - (MS12-049) Microsoft Windows TLS Protocol Information Disclosure (2655992)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1870

[Update Details](#)

Recommendation is updated

**13876 - (MS12-049) Vulnerability in TLS Could Allow Information Disclosure (2655992)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-1870

[Update Details](#)

Recommendation is updated

**14206 - (MS12-066) Microsoft Office HTML Sanitization Privilege Escalation (2741517)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2520

[Update Details](#)

Recommendation is updated

#### **14216 - (MS12-069) Microsoft Kerberos NULL Dereference Denial Of Service (2754673)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2551

[Update Details](#)

Recommendation is updated

#### **14217 - (MS12-069) Vulnerability in Kerberos Could Allow Denial of Service (2743555)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-2551

[Update Details](#)

Recommendation is updated

#### **14577 - (MS13-006) Microsoft Windows SSL And TLS Protocol Security Bypass (2785220)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0013

[Update Details](#)

Recommendation is updated

#### **14580 - (MS13-006) Vulnerability in Microsoft Windows Could Allow Security Feature Bypass (2785220)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0013

[Update Details](#)

Recommendation is updated

#### **14675 - (MS13-016) Vulnerabilities In Windows Kernel-Mode Drivers Could Allow Elevation Of Privilege (2778344)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1248, CVE-2013-1249, CVE-2013-1250, CVE-2013-1251, CVE-2013-1252, CVE-2013-1253, CVE-2013-1254, CVE-2013-1255, CVE-2013-1256, CVE-2013-1257, CVE-2013-1258, CVE-2013-1259, CVE-2013-1260, CVE-2013-1261, CVE-2013-1262, CVE-2013-1263, CVE-2013-1264, CVE-2013-1265, CVE-2013-1266, CVE-2013-1267, CVE-2013-1268, CVE-2013-1269, CVE-2013-1270, CVE-2013-1271, CVE-2013-1272, CVE-2013-1273, CVE-2013-1274, CVE-2013-1275, CVE-2013-1276, CVE-2013-1277

[Update Details](#)

Recommendation is updated

**14680 - (MS13-016) Microsoft Windows Race Condition I Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1248

[Update Details](#)

Recommendation is updated

**14681 - (MS13-016) Microsoft Windows Race Condition II Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1249

[Update Details](#)

Recommendation is updated

**14682 - (MS13-016) Microsoft Windows Race Condition III Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1250

[Update Details](#)

Recommendation is updated

**14683 - (MS13-016) Microsoft Windows Race Condition IV Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1251

[Update Details](#)

Recommendation is updated

**14685 - (MS13-016) Microsoft Windows Race Condition IX Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1256

[Update Details](#)

Recommendation is updated

**14686 - (MS13-016) Microsoft Windows Race Condition V Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1252

[Update Details](#)

Recommendation is updated

**14687 - (MS13-016) Microsoft Windows Race Condition VI Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1253

[Update Details](#)

Recommendation is updated

**14689 - (MS13-016) Microsoft Windows Race Condition VII Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1254

[Update Details](#)

Recommendation is updated

**14691 - (MS13-016) Microsoft Windows Race Condition XXX Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1277

[Update Details](#)

Recommendation is updated

**14692 - (MS13-016) Microsoft Windows Race Condition XXVIII Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1275

[Update Details](#)

Recommendation is updated

#### **14694 - (MS13-016) Microsoft Windows Race Condition XXVII Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1274

#### Update Details

Recommendation is updated

#### **14705 - (MS13-009) Microsoft Internet Explorer Shift JIS Character Encoding Information Disclosure (2792100)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-0015

#### Update Details

Recommendation is updated

#### **14708 - (MS13-016) Microsoft Windows Race Condition VIII Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1255

#### Update Details

Recommendation is updated

#### **14709 - (MS13-016) Microsoft Windows Race Condition X Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1257

#### Update Details

Recommendation is updated

#### **14710 - (MS13-016) Microsoft Windows Race Condition XI Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1258

#### Update Details

Recommendation is updated

#### **14720 - (MS13-016) Microsoft Windows Race Condition XII Privilege Escalation (2778344)**



Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1259

[Update Details](#)

Recommendation is updated

#### **14721 - (MS13-016) Microsoft Windows Race Condition XIII Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1260

[Update Details](#)

Recommendation is updated

#### **14722 - (MS13-016) Microsoft Windows Race Condition XIV Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1261

[Update Details](#)

Recommendation is updated

#### **14723 - (MS13-016) Microsoft Windows Race Condition XIX Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1266

[Update Details](#)

Recommendation is updated

#### **14724 - (MS13-016) Microsoft Windows Race Condition XV Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1262

[Update Details](#)

Recommendation is updated

#### **14725 - (MS13-016) Microsoft Windows Race Condition XVI Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-1263

[Update Details](#)

Recommendation is updated

**14726 - (MS13-016) Microsoft Windows Race Condition XVII Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-1264

[Update Details](#)

Recommendation is updated

**14727 - (MS13-016) Microsoft Windows Race Condition XVIII Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-1265

[Update Details](#)

Recommendation is updated

**14728 - (MS13-016) Microsoft Windows Race Condition XX Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-1267

[Update Details](#)

Recommendation is updated

**14729 - (MS13-016) Microsoft Windows Race Condition XXI Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-1268

[Update Details](#)

Recommendation is updated

**14730 - (MS13-016) Microsoft Windows Race Condition XXII Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-1269

[Update Details](#)

Recommendation is updated

**14731 - (MS13-016) Microsoft Windows Race Condition XXIII Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1270

[Update Details](#)

Recommendation is updated

**14732 - (MS13-016) Microsoft Windows Race Condition XXIV Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1271

[Update Details](#)

Recommendation is updated

**14733 - (MS13-016) Microsoft Windows Race Condition XXIX Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1276

[Update Details](#)

Recommendation is updated

**14734 - (MS13-016) Microsoft Windows Race Condition XXV Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1272

[Update Details](#)

Recommendation is updated

**14736 - (MS13-016) Microsoft Windows Race Condition XXVI Privilege Escalation (2778344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1273

[Update Details](#)

Recommendation is updated

#### **14929 - (MS13-036) Microsoft Windows Kernel Race Condition I Privilege Escalation (2829996)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1283

[Update Details](#)

Recommendation is updated

#### **14931 - (MS13-036) Microsoft Windows Kernel Race Condition II Privilege Escalation (2829996)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1292

[Update Details](#)

Recommendation is updated

#### **14932 - (MS13-036) Microsoft Windows Kernel NTFS Pointer Dereference Privilege Escalation (2829996)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1293

[Update Details](#)

Recommendation is updated

#### **14933 - (MS13-031) Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2813170)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1284, CVE-2013-1294

[Update Details](#)

Recommendation is updated

#### **14935 - (MS13-031) Microsoft Windows Kernel Race Condition I Privilege Escalation (2813170)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1284

[Update Details](#)

Recommendation is updated

#### **14936 - (MS13-031) Microsoft Windows Kernel Race Condition II Privilege Escalation (2813170)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1294

##### Update Details

Recommendation is updated

#### **14944 - (MS13-035) Microsoft Server Software And Office Apps HTML Sanitization Privilege Escalation (2821818)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1289

##### Update Details

Recommendation is updated

#### **14945 - (MS13-035) Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege (2821818)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1289

##### Update Details

Recommendation is updated

#### **15182 - (MS13-048) Microsoft Windows Kernel Information Disclosure (2839229)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3136

##### Update Details

Recommendation is updated

#### **15183 - (MS13-048) Vulnerability in Windows Kernel Could Allow Information Disclosure (2839229)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3136

##### Update Details

Recommendation is updated

#### **15257 - (MS13-053) Microsoft Windows Kernel Buffer Overflow Remote Code Execution (2850851)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3172

[Update Details](#)

Recommendation is updated

**15371 - (MS13-063) Microsoft Windows Kernel Memory Corruption III Remote Code Execution (2859537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3198

[Update Details](#)

Recommendation is updated

**15372 - (MS13-063) Microsoft Windows Kernel Memory Corruption II Remote Code Execution (2859537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3197

[Update Details](#)

Recommendation is updated

**15373 - (MS13-063) Microsoft Windows Kernel Memory Corruption I Remote Code Execution (2859537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3196

[Update Details](#)

Recommendation is updated

**15374 - (MS13-063) Microsoft Windows Kernel ASLR Security Bypass (2859537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-2556

[Update Details](#)

Recommendation is updated

**15536 - (MS13-072) Microsoft Office XML External Entities Resolution Information Disclosure (2845537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3160

[Update Details](#)

Recommendation is updated

**15541 - (MS13-067) Microsoft SharePoint Denial of Service (2834052)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-0081

[Update Details](#)

Recommendation is updated

**15543 - (MS13-067) Microsoft SharePoint Cross-Site Scripting Privilege Escalation (2834052)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3179

[Update Details](#)

Recommendation is updated

**15544 - (MS13-067) Microsoft SharePoint POST Cross-Site Scripting Privilege Escalation (2834052)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3180

[Update Details](#)

Recommendation is updated

**15549 - (MS13-067) Microsoft SharePoint Office Memory Corruption I Remote Code Execution (2834052)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-1315

[Update Details](#)

Recommendation is updated

**15550 - (MS13-067) Microsoft SharePoint Word Memory Corruption I Remote Code Execution (2834052)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3847

[Update Details](#)

Recommendation is updated

**15551 - (MS13-067) Microsoft SharePoint Word Memory Corruption II Remote Code Execution (2834052)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3848

[Update Details](#)

Recommendation is updated

**15552 - (MS13-067) Microsoft SharePoint Word Memory Corruption III Remote Code Execution (2834052)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3849

[Update Details](#)

Recommendation is updated

**15553 - (MS13-067) Microsoft SharePoint Word Memory Corruption IV Remote Code Execution (2834052)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3857

[Update Details](#)

Recommendation is updated

**15554 - (MS13-067) Microsoft SharePoint Word Memory Corruption V Remote Code Execution (2834052)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3858

[Update Details](#)

Recommendation is updated

**15557 - (MS13-072) Microsoft Office Word Memory Corruption I Remote Code Execution (2845537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3847

[Update Details](#)



Recommendation is updated

#### **15559 - (MS13-072) Microsoft Office Word Memory Corruption II Remote Code Execution (2845537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3848

[Update Details](#)

Recommendation is updated

#### **15560 - (MS13-072) Microsoft Office Word Memory Corruption III Remote Code Execution (2845537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3849

[Update Details](#)

Recommendation is updated

#### **15561 - (MS13-072) Microsoft Office Word Memory Corruption IV Remote Code Execution (2845537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3850

[Update Details](#)

Recommendation is updated

#### **15563 - (MS13-072) Microsoft Office Word Memory Corruption V Remote Code Execution (2845537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3851

[Update Details](#)

Recommendation is updated

#### **15564 - (MS13-072) Microsoft Office Word Memory Corruption VI Remote Code Execution (2845537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3852

[Update Details](#)

Recommendation is updated

### **15565 - (MS13-072) Microsoft Office Word Memory Corruption VII Remote Code Execution (2845537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3853

#### Update Details

Recommendation is updated

### **15566 - (MS13-072) Microsoft Office Word Memory Corruption VIII Remote Code Execution (2845537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3854

#### Update Details

Recommendation is updated

### **15567 - (MS13-072) Microsoft Office Word Memory Corruption IX Remote Code Execution (2845537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3855

#### Update Details

Recommendation is updated

### **15568 - (MS13-072) Microsoft Office Word Memory Corruption X Remote Code Execution (2845537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3856

#### Update Details

Recommendation is updated

### **15570 - (MS13-072) Microsoft Office Word Memory Corruption XI Remote Code Execution (2845537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3857

#### Update Details

Recommendation is updated

### **15571 - (MS13-072) Microsoft Office Word Memory Corruption XII Remote Code Execution (2845537)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3858

[Update Details](#)

Recommendation is updated

#### **15579 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation I (2876315)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1341

[Update Details](#)

Recommendation is updated

#### **15580 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation II (2876315)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1342

[Update Details](#)

Recommendation is updated

#### **15581 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation III (2876315)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1343

[Update Details](#)

Recommendation is updated

#### **15582 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation IV (2876315)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-1344

[Update Details](#)

Recommendation is updated

#### **15583 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation V (2876315)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3864

[Update Details](#)

Recommendation is updated

**15584 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation VI (2876315)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3865

[Update Details](#)

Recommendation is updated

**15585 - (MS13-076) Microsoft Win32k Kernel-Mode Drivers Privilege Escalation VII (2876315)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3866

[Update Details](#)

Recommendation is updated

**15587 - (MS13-077) Microsoft Windows Service Control Manager Double Free Privilege Escalation (2872339)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3862

[Update Details](#)

Recommendation is updated

**15589 - (MS13-077) Microsoft Windows Service Control Manager Double Free Privilege Escalation (2872339)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3862

[Update Details](#)

Recommendation is updated

**15706 - (MS13-080) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2879017)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3872

[Update Details](#)

Recommendation is updated

**15707 - (MS13-080) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2879017)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3873

[Update Details](#)

Recommendation is updated

**15708 - (MS13-080) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2879017)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3874

[Update Details](#)

Recommendation is updated

**15709 - (MS13-080) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2879017)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3875

[Update Details](#)

Recommendation is updated

**15710 - (MS13-080) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2879017)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3882

[Update Details](#)

Recommendation is updated

**15712 - (MS13-080) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2879017)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3885

[Update Details](#)

Recommendation is updated

#### **15713 - (MS13-080) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2879017)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3886

[Update Details](#)

Recommendation is updated

#### **15714 - (MS13-087) Microsoft Silverlight Information Disclosure (2890788)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3896

[Update Details](#)

Recommendation is updated

#### **15715 - (MS13-080) Microsoft Internet Explorer Memory Corruption IX Remote Code Execution (2879017)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3897

[Update Details](#)

Recommendation is updated

#### **15716 - (MS13-080) Microsoft Internet Explorer Memory Corruption X Remote Code Execution (2879017)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3893

[Update Details](#)

Recommendation is updated

#### **15722 - (MS13-084) Microsoft SharePoint Excel Remote Code Execution (2885089)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3889

[Update Details](#)

Recommendation is updated

### **15723 - (MS13-084) Microsoft SharePoint Parameter Injection Privilege escalation (2885089)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3895

#### Update Details

Recommendation is updated

### **15730 - (MS13-082) Microsoft .NET Framework JSON Parsing Denial of Service (2878890)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3861

#### Update Details

Recommendation is updated

### **15731 - (MS13-082) Microsoft .NET Framework Entity Expansion Denial of Service (2878890)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3860

#### Update Details

Recommendation is updated

### **15732 - (MS13-082) Microsoft .NET Framework OpenType Font Remote Code Execution (2878890)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3128

#### Update Details

Recommendation is updated

### **15735 - (MS13-081) Microsoft Windows DirectX Graphics Kernel Subsystem Double Fetch Privilege Escalation (2870008)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3888

#### Update Details

Recommendation is updated

### **15736 - (MS13-081) Microsoft Windows Win32k NULL Page Privilege Escalation (2870008)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3881

[Update Details](#)

Recommendation is updated

**15737 - (MS13-081) Microsoft Windows App Container Privilege Escalation (2870008)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3880

[Update Details](#)

Recommendation is updated

**15738 - (MS13-081) Microsoft Windows Win32k Use After Free Privilege Escalation (2870008)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3879

[Update Details](#)

Recommendation is updated

**15739 - (MS13-081) Microsoft Windows USB Descriptor Privilege Escalation (2870008)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3200

[Update Details](#)

Recommendation is updated

**15907 - (MS13-095) Microsoft Windows XML Digital Signatures Denial of Service (2868626)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3869

[Update Details](#)

Recommendation is updated

**15908 - (MS13-095) Vulnerability in XML Digital Signatures Could Allow Denial of Service (2868626)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)



Risk Level: Medium  
CVE: CVE-2013-3869

[Update Details](#)

Recommendation is updated

**15917 - (MS13-088) Microsoft Internet Explorer CSS Characters Information Disclosure (2888505)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3909

[Update Details](#)

Recommendation is updated

**15918 - (MS13-088) Microsoft Internet Explorer Memory Corruption I Remote Code Execution (2888505)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3910

[Update Details](#)

Recommendation is updated

**15919 - (MS13-088) Microsoft Internet Explorer Memory Corruption II Remote Code Execution (2888505)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3911

[Update Details](#)

Recommendation is updated

**15920 - (MS13-088) Microsoft Internet Explorer Memory Corruption III Remote Code Execution (2888505)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3912

[Update Details](#)

Recommendation is updated

**15921 - (MS13-088) Microsoft Internet Explorer Memory Corruption IV Remote Code Execution (2888505)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3914

[Update Details](#)

Recommendation is updated

**15922 - (MS13-088) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (2888505)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3915

[Update Details](#)

Recommendation is updated

**15923 - (MS13-088) Microsoft Internet Explorer Memory Corruption VI Remote Code Execution (2888505)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3916

[Update Details](#)

Recommendation is updated

**15924 - (MS13-088) Microsoft Internet Explorer Memory Corruption VII Remote Code Execution (2888505)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3917

[Update Details](#)

Recommendation is updated

**15925 - (MS13-088) Microsoft Internet Explorer Memory Corruption VIII Remote Code Execution (2888505)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3871

[Update Details](#)

Recommendation is updated

**15926 - (MS13-088) Microsoft Internet Explorer Print Preview Information Disclosure (2888505)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3908

[Update Details](#)

Recommendation is updated

#### **16021 - (MS13-097) Microsoft Internet Explorer Memory Corruption I Privilege Escalation (2898785)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5045

[Update Details](#)

Recommendation is updated

#### **16022 - (MS13-097) Microsoft Internet Explorer Memory Corruption II Privilege Escalation (2898785)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5046

[Update Details](#)

Recommendation is updated

#### **16033 - (MS13-101) Microsoft Windows Integer Overflow I Privilege Escalation (2880430)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3899

[Update Details](#)

Recommendation is updated

#### **16034 - (MS13-101) Microsoft Windows Use-After-Free Privilege Escalation (2880430)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3902

[Update Details](#)

Recommendation is updated

#### **16035 - (MS13-101) Microsoft Windows TrueType Font Parsing Privilege Escalation (2880430)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3903

[Update Details](#)

Recommendation is updated

### **16036 - (MS13-101) Microsoft Windows Port-Class Driver Double Fetch Privilege Escalation (2880430)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-3907

#### Update Details

Recommendation is updated

### **16037 - (MS13-101) Microsoft Windows Integer Overflow II Privilege Escalation (2880430)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2013-5058

#### Update Details

Recommendation is updated

### **16208 - (MS14-003) Microsoft Windows Kernel-Mode Drivers Privilege Elevation (2913602)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0262

#### Update Details

Recommendation is updated

### **16290 - (MS14-010) Microsoft Internet Explorer Memory Corruption Privilege Escalation (2909921)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0268

#### Update Details

Recommendation is updated

### **16312 - (MS14-010) Microsoft Internet Explorer Cross Domain Information Disclosure (2909921)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0293

#### Update Details

Recommendation is updated

### **16318 - (MS14-009) Microsoft .NET Address Space Layout Randomization Security Bypass (2916607)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0295

[Update Details](#)

Recommendation is updated

**16319 - (MS14-009) Microsoft .NET POST Request Denial of Service (2916607)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0253

[Update Details](#)

Recommendation is updated

**16320 - (MS14-009) Microsoft .NET Type Traversal Privilege Escalation (2916607)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0257

[Update Details](#)

Recommendation is updated

**16497 - (MS14-019) Microsoft Windows File Handling Remote Code Execution (2922229)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-0315

[Update Details](#)

Recommendation is updated

**16601 - (MS14-026) Vulnerability in .NET could allow Remote Code Execution (2958732)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-1806

[Update Details](#)

Recommendation is updated

**16611 - (MS14-027) Vulnerability in Windows Shell Handler Could Allow Elevation of Privilege (2962488)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2014-1807

[Update Details](#)

Recommendation is updated

**16612 - (MS14-027) Microsoft Windows Shell Handler File Association Privilege Escalation (2962488)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

**16709 - (MS14-034) Microsoft Word Embedded Font Remote Code Execution (2969261)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2014-2778

[Update Details](#)

Recommendation is updated

**16733 - (MS14-035) Microsoft Internet Explorer Privilege Escalation I (2969262)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2014-1764

[Update Details](#)

Recommendation is updated

**16738 - (MS14-035) Microsoft Internet Explorer Privilege Escalation III (2969262)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2014-2777

[Update Details](#)

Recommendation is updated

**16744 - (MS14-035) Microsoft Internet Explorer Information Disclosure (2969262)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2014-1777

[Update Details](#)

Recommendation is updated

**17104 - (MS14-053) Vulnerability in .NET Framework Could Allow Denial of Service (2990931)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4072

[Update Details](#)

Recommendation is updated

**17105 - (MS14-053) Microsoft .NET Framework ASP.NET Hash Collision Denial of Service (2990931)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-4072

[Update Details](#)

Recommendation is updated

**17365 - (MS14-065) Microsoft Internet Explorer ASLR Security Bypass (3003057)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-6339

[Update Details](#)

Recommendation is updated

**17509 - (MS14-080) Microsoft Internet Explorer XSS Filter I Security Bypass (3008923)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-6328

[Update Details](#)

Recommendation is updated

**17510 - (MS14-080) Microsoft Internet Explorer XSS Filter II Security Bypass (3008923)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-6365

[Update Details](#)

Recommendation is updated

#### **17824 - (MS15-009) Microsoft Internet Explorer ASLR Security Bypass I (3034682)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0051

[Update Details](#)

Recommendation is updated

#### **17827 - (MS15-009) Microsoft Internet Explorer Privilege Escalation I (3034682)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0054

[Update Details](#)

Recommendation is updated

#### **17828 - (MS15-009) Microsoft Internet Explorer Privilege Escalation II (3034682)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0055

[Update Details](#)

Recommendation is updated

#### **17832 - (MS15-009) Microsoft Internet Explorer ASLR Security Bypass II (3034682)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0069

[Update Details](#)

Recommendation is updated

#### **17833 - (MS15-009) Microsoft Internet Explorer Cross-Domain Information Disclosure (3034682)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0070

[Update Details](#)

Recommendation is updated



### **17834 - (MS15-009) Microsoft Internet Explorer ASLR Security Bypass III (3034682)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0071

#### Update Details

Recommendation is updated

### **17979 - (MS15-027) Microsoft Windows NETLOGON Information Disclosure (3002657)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0005

#### Update Details

Recommendation is updated

### **17984 - (MS15-022) Microsoft Office Sharepoint Cross-Site Scripting Privilege Escalation II (3038999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1636

#### Update Details

Recommendation is updated

### **17985 - (MS15-022) Microsoft Office Sharepoint Cross-Site Scripting Privilege Escalation I (3038999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1633

#### Update Details

Recommendation is updated

### **17986 - (MS15-022) Microsoft Office World Local Zone Remote Code Execution (3038999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0097

#### Update Details

Recommendation is updated

### **17988 - (MS15-022) Microsoft Office Memory Handling Remote Code Execution (3038999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0085

[Update Details](#)

Recommendation is updated

**17997 - (MS15-027) Vulnerability in NETLOGON Could Allow Spoofing (3002657)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0005

[Update Details](#)

Recommendation is updated

**18012 - (MS15-018) Microsoft Internet Explorer Memory Corruption I Privilege Escalation (3032359)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0072

[Update Details](#)

Recommendation is updated

**18014 - (MS15-018) Microsoft Internet Explorer Memory Corruption II Privilege Escalation (3032359)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1627

[Update Details](#)

Recommendation is updated

**18025 - (MS15-023) Microsoft Windows Kernel Calling Thread Privilege Escalation (3034344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0078

[Update Details](#)

Recommendation is updated

**18026 - (MS15-023) Microsoft Windows Kernel Memory I Information Disclosure (3034344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-0077

[Update Details](#)

Recommendation is updated

**18027 - (MS15-023) Microsoft Windows Kernel Memory II Information Disclosure (3034344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-0094

[Update Details](#)

Recommendation is updated

**18028 - (MS15-023) Microsoft Windows Kernel Memory III Information Disclosure (3034344)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-0095

[Update Details](#)

Recommendation is updated

**18030 - (MS15-025) Microsoft Office Kernel Impersonation Level Check Privilege Escalation (3038680)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-0075

[Update Details](#)

Recommendation is updated

**18031 - (MS15-025) Microsoft Windows Registry Virtualization Privilege Escalation (3038680)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-0073

[Update Details](#)

Recommendation is updated

**18041 - (MS15-031) Vulnerability in Schannel Could Allow Security Feature Bypass (3046015)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-1637

[Update Details](#)

Recommendation is updated

**18043 - (MS15-031) Microsoft Windows Schannel Security Bypass (3046049)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1637

[Update Details](#)

Recommendation is updated

**18142 - (MS15-032) Microsoft Internet Explorer Memory Corruption V Remote Code Execution (3038314)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1661

[Update Details](#)

Recommendation is updated

**18164 - (MS15-041) Vulnerability in .NET Framework Could Allow Information Disclosure (3048010)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1648

[Update Details](#)

Recommendation is updated

**18165 - (MS15-041) Microsoft .NET Framework Information Disclosure (3048010)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1648

[Update Details](#)

Recommendation is updated

**18171 - (MS15-038) Microsoft Windows MS-DOS Device Name Privilege Escalation (3049576)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1644

[Update Details](#)

Recommendation is updated

#### **18187 - (MS15-033) Microsoft Outlook Mac App Cross-Site Scripting (3048019)**

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2015-1639

[Update Details](#)

Recommendation is updated

#### **18265 - (MS15-046) Microsoft Office Memory Corruption I Remote Code Execution (3057181)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1682

[Update Details](#)

Recommendation is updated

#### **18267 - (MS15-046) Microsoft Office Memory Corruption I Remote Code Execution (3057181)**

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-1682

[Update Details](#)

Recommendation is updated

#### **18272 - (MS15-048) Microsoft .NET Framework Forms Application Privilege Escalation (3057134)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1673

[Update Details](#)

Recommendation is updated

#### **18274 - (MS15-048) Microsoft .NET Framework XML Decryption Denial of Service (3057134)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1672

[Update Details](#)

Recommendation is updated

#### **18278 - (MS15-055) Microsoft Windows Schannel Information Disclosure (3061518)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1716

Update Details

Recommendation is updated

**18305 - (MS15-044) Microsoft Windows GDI+ OpenType Font Parsing Remote Code Execution (3057110)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1670

Update Details

Recommendation is updated

**18311 - (MS15-055) Vulnerability in Schannel Could Allow Information Disclosure (3061518)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1716

Update Details

Recommendation is updated

**18469 - (MS15-061) Microsoft Windows Kernel Object Use-After-Free Privilege Escalation (3057839)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1724

Update Details

Recommendation is updated

**18650 - (MS15-070) Microsoft Office Memory Corruption VI Remote Code Execution (3072620)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2424

Update Details

Recommendation is updated

**18921 - (MS15-101) Microsoft .NET Framework MVC Denial of Service (3089662)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-2526

[Update Details](#)

Recommendation is updated

**18932 - (MS15-094) Microsoft Internet Explorer Memory Handling I Information Disclosure (3089548)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-2483

[Update Details](#)

Recommendation is updated

**19072 - (MS15-107) Microsoft Edge Memory Information Disclosure I (3096448)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-6057

[Update Details](#)

Recommendation is updated

**19075 - (MS15-107) Cumulative Security Update for Microsoft Edge (3096448)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-6057, CVE-2015-6058

[Update Details](#)

Recommendation is updated

**19094 - (MS15-106) Microsoft Internet Explorer III Information Disclosure (3096441)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-6053

[Update Details](#)

Recommendation is updated

**19268 - (MS15-121) Microsoft Windows Schannel Triple Handshake Spoofing Information Disclosure (3081320)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-6112

[Update Details](#)

Recommendation is updated

**19269 - (MS15-121) Security Update for Schannel to Address Spoofing (3081320)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6112

[Update Details](#)

Recommendation is updated

**19335 - (MS15-128) Microsoft Windows Graphics Memory Corruption Remote Code Execution I (3104503)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6106

[Update Details](#)

Recommendation is updated

**19355 - (MS15-124) Microsoft Internet Explorer Script Engine Information Disclosure (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6135

[Update Details](#)

Recommendation is updated

**19384 - (MS15-126) Microsoft JScript and VBScript Engine Information Disclosure (3116178)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6135

[Update Details](#)

Recommendation is updated

**19385 - (MS15-124) Microsoft Internet Explorer XSS Filter Policies Enforcement Security Bypass (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6164

[Update Details](#)



Recommendation is updated

#### **19403 - (MS15-125) Microsoft Edge Browser Content Privilege Escalation (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6139

[Update Details](#)

Recommendation is updated

#### **19412 - (MS15-125) Microsoft Edge ASLR Security Bypass (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6161

[Update Details](#)

Recommendation is updated

#### **19414 - (MS15-125) Microsoft Edge Spoofing Information Disclosure (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6169

[Update Details](#)

Recommendation is updated

#### **19415 - (MS15-125) Microsoft Edge Permissions Scripts Privilege Escalation (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6170

[Update Details](#)

Recommendation is updated

#### **19416 - (MS15-125) Microsoft Edge XSS Filter Information Disclosure (3116184)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6176

[Update Details](#)

Recommendation is updated

### **19510 - (MS16-005) Microsoft Windows GDI32.dll ASLR Bypass Information Disclosure (3124584)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0008

#### Update Details

Recommendation is updated

### **19514 - (MS16-007) Microsoft Windows MAPI DLL Loading Privilege Escalation (3124901)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0020

#### Update Details

Recommendation is updated

### **19515 - (MS16-007) Microsoft Windows Remote Desktop Protocol Remote Logon Security Bypass (3124901)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0019

#### Update Details

Recommendation is updated

### **19516 - (MS16-007) Microsoft Windows DLL Loading Input Validating Remote Code Execution II (3124901)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0018

#### Update Details

Recommendation is updated

### **19517 - (MS16-007) Microsoft Windows DLL Loading Input Validating Remote Code Execution I (3124901)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0016

#### Update Details

Recommendation is updated

### **19518 - (MS16-007) Microsoft Windows DirectShow Heap Corruption Remote Code Execution (3124901)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0015

[Update Details](#)

Recommendation is updated

**19519 - (MS16-007) Microsoft Windows DLL Loading Privilege Escalation (3124901)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0014

[Update Details](#)

Recommendation is updated

**19524 - (MS16-001) Microsoft Internet Explorer Cross Domain Privilege Escalation (3124903)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0005

[Update Details](#)

Recommendation is updated

**19527 - (MS16-004) Microsoft SharePoint Access Control Policy Security Bypass I (3124585)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0011

[Update Details](#)

Recommendation is updated

**19528 - (MS16-004) Microsoft SharePoint Access Control Policy Security Bypass II (3124585)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6117

[Update Details](#)

Recommendation is updated

**19529 - (MS16-004) Microsoft Office ASLR Security Bypass (3124585)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-0012

[Update Details](#)

Recommendation is updated

**19542 - (MS16-008) Microsoft Windows Kernel TOCTOU Privilege Escalation I (3124605)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-0006

[Update Details](#)

Recommendation is updated

**19543 - (MS16-008) Microsoft Windows Kernel TOCTOU Privilege Escalation II (3124605)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-0007

[Update Details](#)

Recommendation is updated

**19637 - (MS16-019) Security Update for .NET Framework to Address Denial of Service (3137893)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-0033, CVE-2016-0047

[Update Details](#)

Recommendation is updated

**19638 - (MS16-019) Microsoft Windows Forms Information Disclosure (3137893)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-0047

[Update Details](#)

Recommendation is updated

**19639 - (MS16-019) Microsoft .NET Framework Stack Overflow Denial of Service (3137893)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-0033

[Update Details](#)

Recommendation is updated

**19667 - (MS16-014) Microsoft Windows DLL Loading Denial of Service (3134228)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0044

[Update Details](#)

Recommendation is updated

**19670 - (MS16-021) Microsoft RADIUS Server Denial of Service (3133043)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0050

[Update Details](#)

Recommendation is updated

**19675 - (MS16-021) Security Update for NPS RADIUS Server to Address Denial of Service (3133043)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0050

[Update Details](#)

Recommendation is updated

**19678 - (MS16-009) Microsoft Internet Explorer DLL Loading Remote Code Execution (3134220)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0041

[Update Details](#)

Recommendation is updated

**19736 - (MS16-029) Microsoft Office Memory Corruption Remote Code Execution I (3141806)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0021

[Update Details](#)

Recommendation is updated

#### **19737 - (MS16-029) Microsoft Office Invalid Signed Library Security Bypass (3141806)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0057

[Update Details](#)

Recommendation is updated

#### **19738 - (MS16-029) Microsoft Office Memory Corruption Remote Code Execution II (3141806)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0134

[Update Details](#)

Recommendation is updated

#### **19739 - (MS16-031) Security Update for Microsoft Windows to Address Elevation of Privilege (3140410)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0087

[Update Details](#)

Recommendation is updated

#### **19740 - (MS16-031) Microsoft Windows User Impersonation Privilege Escalation (3140410)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0087

[Update Details](#)

Recommendation is updated

#### **19748 - (MS16-032) Microsoft Windows Secondary Logon Memory Handlers Privilege Escalation (3143141)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0099

[Update Details](#)

Recommendation is updated

### **19749 - (MS16-033) Microsoft Windows USB Mass Storage Class Driver Privilege Escalation (3143142)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0133

#### Update Details

Recommendation is updated

### **19751 - (MS16-034) Microsoft Windows Kernel Privilege Escalation I (3143145)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0093

#### Update Details

Recommendation is updated

### **19752 - (MS16-034) Microsoft Windows Kernel Privilege Escalation II (3143145)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0094

#### Update Details

Recommendation is updated

### **19754 - (MS16-034) Microsoft Windows Kernel Privilege Escalation III (3143145)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0095

#### Update Details

Recommendation is updated

### **19755 - (MS16-034) Microsoft Windows Kernel Privilege Escalation IV (3143145)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0096

#### Update Details

Recommendation is updated

### **19757 - (MS16-035) Microsoft .NET Framework XML Validation Security Bypass (3141780)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0132

Update Details

Recommendation is updated

**19761 - (MS16-032) Security Update for Secondary Logon to Address Elevation of Privilege (3143141)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0099

Update Details

Recommendation is updated

**19762 - (MS16-033) Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege (3143142)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0133

Update Details

Recommendation is updated

**19764 - (MS16-035) Security Update for .NET Framework to Address Security Feature Bypass (3141780)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0132

Update Details

Recommendation is updated

**19767 - (MS16-024) Microsoft Edge Referrer Policy Information Disclosure (3142019)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0125

Update Details

Recommendation is updated

**19785 - (MS16-030) Microsoft Windows OLE User Input Validation Remote Code Execution I (3143136)**

Category: Windows Host Assessment -> Patches and Hotfixes



(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0091

[Update Details](#)

Recommendation is updated

#### **19786 - (MS16-030) Microsoft Windows OLE User Input Validation Remote Code Execution II (3143136)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0092

[Update Details](#)

Recommendation is updated

#### **19901 - (MS16-048) Security Update for CSRSS (3148528)**

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0151

[Update Details](#)

Recommendation is updated

#### **19907 - (MS16-039) Microsoft Windows Win32k Graphics Privilege Escalation I (3148522)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0143

[Update Details](#)

Recommendation is updated

#### **19908 - (MS16-039) Microsoft Windows Win32k Graphics Privilege Escalation II (3148522)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0165

[Update Details](#)

Recommendation is updated

#### **19916 - (MS16-038) Microsoft Edge Javascript Privilege Escalation (3148532)**

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0161

[Update Details](#)

Recommendation is updated

**19917 - (MS16-049) Security Update for HTTP.sys (3148795)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0150

[Update Details](#)

Recommendation is updated

**19918 - (MS16-046) Security Update for Secondary Logon (3148538)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0135

[Update Details](#)

Recommendation is updated

**19919 - (MS16-045) Microsoft Windows Hyper-V Information Disclosure II (3143118)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0090

[Update Details](#)

Recommendation is updated

**19920 - (MS16-045) Microsoft Windows Hyper-V Information Disclosure I (3143118)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0089

[Update Details](#)

Recommendation is updated

**19921 - (MS16-045) Microsoft Windows Hyper-V Remote Code Execution (3143118)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0088

[Update Details](#)

Recommendation is updated

**19923 - (MS16-047) Microsoft Windows RPC Downgrade Privilege Escalation (3148527)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0128

[Update Details](#)

Recommendation is updated

**19924 - (MS16-047) Security Update for SAM and LSAD Remote Protocols (3148527)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0128

[Update Details](#)

Recommendation is updated

**19927 - (MS16-041) Security Update for .NET Framework (3148789)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0148

[Update Details](#)

Recommendation is updated

**19928 - (MS16-041) Microsoft .NET Framework Remote Code Execution (3148789)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0148

[Update Details](#)

Recommendation is updated

**19929 - (MS16-042) Microsoft Office Memory Corruption Remote Code Execution I (3148775)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0122

[Update Details](#)

Recommendation is updated

#### **19931 - (MS16-042) Microsoft Office Memory Corruption Remote Code Execution III (3148775)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0136

[Update Details](#)

Recommendation is updated

#### **19933 - (MS16-042) Microsoft Office Memory Corruption Remote Code Execution IV (3148775)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0139

[Update Details](#)

Recommendation is updated

#### **19934 - (MS16-046) Microsoft Windows Secondary Logon Privilege Escalation (3148538)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0135

[Update Details](#)

Recommendation is updated

#### **19935 - (MS16-049) Microsoft Windows IIS Denial of Service (3148795)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0150

[Update Details](#)

Recommendation is updated

#### **19941 - (MS16-037) Microsoft Internet Explorer JavaScript Information Disclosure (3148531)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0162

[Update Details](#)

Recommendation is updated

---

### **20136 - (MS16-075) Security Update for Windows SMB Server (3164038)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3225

#### Update Details

Recommendation is updated

### **20137 - (MS16-075) Microsoft Windows SMB Server Privilege Escalation (3164038)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3225

#### Update Details

Recommendation is updated

### **20141 - (MS16-077) Microsoft Windows WPAD Proxy Discovery Privilege Escalation (3165191)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3236

#### Update Details

Recommendation is updated

### **20142 - (MS16-077) Microsoft Windows WPAD Privilege Escalation (3165191)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3213

#### Update Details

Recommendation is updated

### **20146 - (MS16-080) Microsoft Windows PDF Remote Code Execution (3164302)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3203

#### Update Details

Recommendation is updated

### **20147 - (MS16-080) Microsoft Windows PDF Information Disclosure II (3164302)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3215

Update Details

Recommendation is updated

**20148 - (MS16-080) Microsoft Windows PDF Information Disclosure I (3164302)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3201

Update Details

Recommendation is updated

**20149 - (MS16-068) Microsoft Edge Content Security Policy Security Bypass (3163656)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3198

Update Details

Recommendation is updated

**20151 - (MS16-068) Microsoft Edge PDF Information Disclosure (3163656)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3201

Update Details

Recommendation is updated

**20156 - (MS16-068) Microsoft Edge PDF Information Disclosure II (3163656)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3215

Update Details

Recommendation is updated

**20158 - (MS16-070) Microsoft Office OLE DLL Side Loading Remote Code Execution (3163610)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3235

[Update Details](#)

Recommendation is updated

**20159 - (MS16-070) Microsoft Office Information Disclosure (3163610)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3234

[Update Details](#)

Recommendation is updated

**20160 - (MS16-070) Microsoft Office Memory Corruption Remote Code Execution II (3163610)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3233

[Update Details](#)

Recommendation is updated

**20173 - (MS16-063) Microsoft Internet Explorer Web Proxy Autodiscovery Privilege Escalation (3163649)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3213

[Update Details](#)

Recommendation is updated

**20174 - (MS16-072) Microsoft Windows Group Policy Privilege Escalation (3163622)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3223

[Update Details](#)

Recommendation is updated

**20175 - (MS16-073) Microsoft Windows Win32k Privilege Escalation I (3164028)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3218

[Update Details](#)

Recommendation is updated

**20176 - (MS16-073) Microsoft Windows Win32k Privilege Escalation II (3164028)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3221

[Update Details](#)

Recommendation is updated

**20177 - (MS16-073) Microsoft Windows Virtual PCI Information Disclosure (3164028)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3232

[Update Details](#)

Recommendation is updated

**20178 - (MS16-074) Microsoft Windows Graphics Component Information Disclosure Vulnerability (3164036)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3216

[Update Details](#)

Recommendation is updated

**20179 - (MS16-074) Microsoft Windows Win32K Privilege Escalation (3164036)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3219

[Update Details](#)

Recommendation is updated

**20180 - (MS16-074) Microsoft Windows ATMF.DLL Privilege Escalation (3164036)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3220

[Update Details](#)



Recommendation is updated

#### **20181 - (MS16-082) Windows Search Component Denial of Service Vulnerability (3165270)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3230

##### Update Details

Recommendation is updated

#### **20182 - (MS16-072) Security Update for Group Policy (3163622)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3223

##### Update Details

Recommendation is updated

#### **20183 - (MS16-078) Microsoft Windows Diagnostics Hub Privilege Escalation (3165479)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3231

##### Update Details

Recommendation is updated

#### **20185 - (MS16-082) Security Update for Microsoft Windows Search Component (3165270)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3230

##### Update Details

Recommendation is updated

#### **20188 - (MS16-073) Security Update for Windows Kernel Mode Drivers (3164028)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3218, CVE-2016-3221, CVE-2016-3232

##### Update Details

Recommendation is updated

### **20189 - (MS16-074) Security Update for Microsoft Graphics Component (3164036)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3216, CVE-2016-3219

#### Update Details

Recommendation is updated

### **20280 - (MS16-091) Microsoft .NET Framework XML Parsing Information Disclosure (3170048)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3255

#### Update Details

Recommendation is updated

### **20296 - (MS16-091) Security Update for .NET Framework (3170048)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3255

#### Update Details

Recommendation is updated

### **20375 - (MS16-099) Microsoft Office Memory Corruption Remote Code Execution I (3177451)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3313

#### Update Details

Recommendation is updated

### **20376 - (MS16-099) Microsoft OneNote Information Disclosure II (3177451)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3315

#### Update Details

Recommendation is updated

### **20377 - (MS16-099) Microsoft Office Memory Corruption Remote Code Execution II (3177451)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3316

[Update Details](#)

Recommendation is updated

#### **20378 - (MS16-099) Microsoft Office Memory Corruption Remote Code Execution III (3177451)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3317

[Update Details](#)

Recommendation is updated

#### **20379 - (MS16-099) Microsoft Office Graphics Component Memory Corruption Remote Code Execution (3177451)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3318

[Update Details](#)

Recommendation is updated

#### **20387 - (MS16-096) Microsoft Edge Browser Memory Corruption Remote Code Execution II (3177358)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3293

[Update Details](#)

Recommendation is updated

#### **20391 - (MS16-096) Microsoft Edge Browser Information Disclosure I (3177358)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3326

[Update Details](#)

Recommendation is updated

#### **20392 - (MS16-096) Microsoft Edge Browser Information Disclosure II (3177358)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3327

[Update Details](#)

Recommendation is updated

**20393 - (MS16-096) Microsoft Edge Browser Information Disclosure III (3177358)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3329

[Update Details](#)

Recommendation is updated

**20394 - (MS16-103) Microsoft Windows ActiveSyncProvider Information Disclosure (3182332)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3312

[Update Details](#)

Recommendation is updated

**20397 - (MS16-101) Microsoft Windows Kerberos Privilege Escalation (3178465)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3237

[Update Details](#)

Recommendation is updated

**20399 - (MS16-095) Microsoft Internet Explorer Browser Information Disclosure III (3177356)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3329

[Update Details](#)

Recommendation is updated

**20400 - (MS16-095) Microsoft Internet Explorer Browser Information Disclosure II (3177356)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3327

[Update Details](#)

Recommendation is updated

**20401 - (MS16-095) Microsoft Internet Explorer Browser Information Disclosure I (3177356)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3326

[Update Details](#)

Recommendation is updated

**20403 - (MS16-095) Microsoft Internet Explorer Local File URI Information Disclosure (3177356)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3321

[Update Details](#)

Recommendation is updated

**20411 - (MS16-098) Microsoft Windows Win32k Privilege Escalation IV (3178466)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3311

[Update Details](#)

Recommendation is updated

**20413 - (MS16-098) Microsoft Windows Win32k Privilege Escalation II (3178466)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3309

[Update Details](#)

Recommendation is updated

**20414 - (MS16-098) Microsoft Windows Win32k Privilege Escalation I (3178466)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3308

[Update Details](#)

Recommendation is updated

#### **20415 - (MS16-098) Microsoft Windows Win32k Privilege Escalation III (3178466)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3310

[Update Details](#)

Recommendation is updated

#### **20483 - (MS16-110) Microsoft Windows Memory Corruption Denial of Service (3178467)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3369

[Update Details](#)

Recommendation is updated

#### **20484 - (MS16-110) Microsoft Windows Memory Corruption Remote Code Execution (3178467)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3368

[Update Details](#)

Recommendation is updated

#### **20485 - (MS16-110) Microsoft Windows MSA Login Sessions NTLM Single Sign On Validation Information Disclosure (3178467)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3352

[Update Details](#)

Recommendation is updated

#### **20486 - (MS16-110) Microsoft Windows Permissions Enforcement DLL Loading Privilege Escalation (3178467)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3346

[Update Details](#)

Recommendation is updated

#### **20494 - (MS16-109) Microsoft Silverlight Memory Object Access Remote Code Execution (3182373)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3367

##### Update Details

Recommendation is updated

#### **20495 - (MS16-109) Security Update for Silverlight (3182373)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3367

##### Update Details

Recommendation is updated

#### **20496 - (MS16-109) Security Update for Silverlight (3182373)**

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-3367

##### Update Details

Recommendation is updated

#### **20497 - (MS16-114) Microsoft Windows SMB v1 Chained Commands Remote Code Execution (3185879)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3345

##### Update Details

Recommendation is updated

#### **20498 - (MS16-114) Security Update for Windows SMBv1 Server (3185879)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3345

##### Update Details

Recommendation is updated

#### **20504 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution I (3183043)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3247

[Update Details](#)

Recommendation is updated

**20507 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution IV (3183043)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3297

[Update Details](#)

Recommendation is updated

**20508 - (MS16-105) Microsoft Edge Memory Corruption Remote Code Execution V (3183043)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3330

[Update Details](#)

Recommendation is updated

**20511 - (MS16-105) Microsoft Edge Browser Information Disclosure I (3183043)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3291

[Update Details](#)

Recommendation is updated

**20512 - (MS16-105) Microsoft Edge Browser Information Disclosure II (3183043)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3325

[Update Details](#)

Recommendation is updated

**20513 - (MS16-105) Microsoft Edge Browser Information Disclosure III (3183043)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)



Risk Level: Medium  
CVE: CVE-2016-3351

[Update Details](#)

Recommendation is updated

**20514 - (MS16-105) Microsoft Edge Browser Information Disclosure IV (3183043)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3374

[Update Details](#)

Recommendation is updated

**20515 - (MS16-105) Microsoft Edge Browser Information Disclosure V (3183043)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3370

[Update Details](#)

Recommendation is updated

**20516 - (MS16-112) Security Update for Windows Lock Screen (3178469)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3302

[Update Details](#)

Recommendation is updated

**20517 - (MS16-112) Microsoft Windows Lock Screen Content Loading Privilege Escalation (3178469)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3302

[Update Details](#)

Recommendation is updated

**20518 - (MS16-113) Security Update for Windows Secure Kernel Mode (3185876)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3344

[Update Details](#)

Recommendation is updated

**20519 - (MS16-113) Microsoft Windows Secure Kernel Information Disclosure (3185876)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3344

[Update Details](#)

Recommendation is updated

**20520 - (MS16-106) Microsoft Windows Graphics Component Win32K Privilege Escalation I (3185848)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3348

[Update Details](#)

Recommendation is updated

**20521 - (MS16-106) Microsoft Windows Graphics Component Win32K Privilege Escalation II (3185848)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3349

[Update Details](#)

Recommendation is updated

**20522 - (MS16-106) Microsoft Windows Graphics Component GDI ASLR Bypass Information Disclosure (3185848)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3354

[Update Details](#)

Recommendation is updated

**20523 - (MS16-106) Microsoft Windows Graphics Component GDI Memory Handling Privilege Escalation (3185848)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3355

[Update Details](#)

Recommendation is updated

#### **20525 - (MS16-111) Microsoft Windows Session Object Privilege Escalation I (3186973)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3305

[Update Details](#)

Recommendation is updated

#### **20526 - (MS16-111) Microsoft Windows Session Object Privilege Escalation II (3186973)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3306

[Update Details](#)

Recommendation is updated

#### **20527 - (MS16-111) Microsoft Windows Kernel API User Permissions Privilege Escalation I (3186973)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3371

[Update Details](#)

Recommendation is updated

#### **20528 - (MS16-111) Microsoft Windows Kernel API User Permissions Privilege Escalation II (3186973)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3372

[Update Details](#)

Recommendation is updated

#### **20529 - (MS16-111) Microsoft Windows Kernel API Privilege Escalation (3186973)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3373

[Update Details](#)

Recommendation is updated

### **20535 - (MS16-104) Microsoft Browser Information Disclosure (3183038)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3291

#### Update Details

Recommendation is updated

### **20536 - (MS16-104) Microsoft Internet Explorer Privilege Escalation (3183038)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3292

#### Update Details

Recommendation is updated

### **20538 - (MS16-104) Microsoft Internet Explorer Memory Corruption Remote Code Execution III (3183038)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3297

#### Update Details

Recommendation is updated

### **20539 - (MS16-104) Microsoft Internet Explorer Memory Corruption Remote Code Execution IV (3183038)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3324

#### Update Details

Recommendation is updated

### **20540 - (MS16-104) Microsoft Internet Explorer Information Disclosure I (3183038)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3325

#### Update Details

Recommendation is updated

### **20541 - (MS16-104) Microsoft Internet Explorer Information Disclosure II (3183038)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3351

[Update Details](#)

Recommendation is updated

#### **20542 - (MS16-104) Microsoft Internet Explorer Security Bypass (3183038)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3353

[Update Details](#)

Recommendation is updated

#### **20544 - (MS16-107) Microsoft Office Certificate Export Information Disclosure (3185852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0141

[Update Details](#)

Recommendation is updated

#### **20546 - (MS16-107) Microsoft Office Memory Corruption Remote Code Execution II (3185852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3358

[Update Details](#)

Recommendation is updated

#### **20547 - (MS16-107) Microsoft Office Memory Corruption Remote Code Execution III (3185852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3359

[Update Details](#)

Recommendation is updated

#### **20548 - (MS16-107) Microsoft Office Memory Corruption Remote Code Execution IV (3185852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3360

[Update Details](#)

Recommendation is updated

**20549 - (MS16-107) Microsoft Office Memory Corruption Remote Code Execution V (3185852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3361

[Update Details](#)

Recommendation is updated

**20550 - (MS16-107) Microsoft Office Memory Corruption Remote Code Execution VI (3185852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3362

[Update Details](#)

Recommendation is updated

**20551 - (MS16-107) Microsoft Office Memory Corruption Remote Code Execution VII (3185852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3363

[Update Details](#)

Recommendation is updated

**20552 - (MS16-107) Microsoft Office Memory Corruption Remote Code Execution IX (3185852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3365

[Update Details](#)

Recommendation is updated

**20553 - (MS16-107) Microsoft Office MIME Attachment Spoofing Security Bypass (3185852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2016-3366

[Update Details](#)

Recommendation is updated

**20554 - (MS16-107) Microsoft Office Memory Corruption Remote Code Execution X (3185852)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3381

[Update Details](#)

Recommendation is updated

**144904 - SuSE Linux 13.2 openSUSE-SU-2016:2443-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> SuSE Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6323

[Update Details](#)

Risk is updated

**188988 - Fedora Linux 22 FEDORA-2015-2673 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2015-2080

[Update Details](#)

Risk is updated

**191004 - Fedora Linux 24 FEDORA-2016-5f050a0a6d Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6323

[Update Details](#)

Risk is updated

**191029 - Fedora Linux 25 FEDORA-2016-57cba655d5 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6323

[Update Details](#)

Risk is updated

**191062 - Fedora Linux 23 FEDORA-2016-87dde780b8 Update Is Not Installed**

---

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-6323

[Update Details](#)

Risk is updated

#### **9697 - (MS10-048) Microsoft Windows Win32k Pool Overflow Vulnerability (2160329)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1887

[Update Details](#)

Recommendation is updated

#### **9698 - (MS10-048) Microsoft Windows Win32k Bounds Checking Vulnerability (2160329)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2010-1887

[Update Details](#)

Recommendation is updated

#### **12251 - (MS11-037) Microsoft MHTML Mime-Formatted Request Could Allow Information Disclosure (2544893)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2011-1894

[Update Details](#)

Recommendation is updated

#### **13404 - (MS12-019) Microsoft Windows DirectWrite Application Denial of Service (2665364)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2012-0156

[Update Details](#)

Recommendation is updated

#### **13407 - (MS12-019) Vulnerability in DirectWrite Could Allow Denial of Service (2665364)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)



Risk Level: Medium  
CVE: CVE-2012-0156

[Update Details](#)

Recommendation is updated

**14205 - (MS12-066) Vulnerabilities in HTML Sanitization Component Could Allow Elevation of Privilege (2741517)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2012-2520

[Update Details](#)

Recommendation is updated

**15711 - (MS13-087) Vulnerability in Silverlight Could Allow Information Disclosure (2890788)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2013-3896

[Update Details](#)

Recommendation is updated

**15717 - (MS13-087) Vulnerability in Silverlight Could Allow Information Disclosure (2890788)**

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: Medium  
CVE: CVE-2013-3896

[Update Details](#)

Recommendation is updated

**17224 - (MS14-057) Microsoft .NET Framework Address Space Layout Randomization Security Bypass (3000414)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2014-4122

[Update Details](#)

Recommendation is updated

**17367 - (MS14-065) Microsoft Internet Explorer Clipboard Information Disclosure (3003057)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2014-6323

[Update Details](#)

Recommendation is updated

**17368 - (MS14-065) Microsoft Internet Explorer Cross-Domain Information Disclosure I (3003057)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-6340

[Update Details](#)

Recommendation is updated

**17370 - (MS14-065) Microsoft Internet Explorer Cross-Domain Information Disclosure II (3003057)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-6345

[Update Details](#)

Recommendation is updated

**17371 - (MS14-065) Microsoft Internet Explorer Cross-Domain Information Disclosure III (3003057)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-6346

[Update Details](#)

Recommendation is updated

**17382 - (MS14-065) Microsoft Internet Explorer Permission Validation I Privilege Escalation (3003057)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-6349

[Update Details](#)

Recommendation is updated

**17383 - (MS14-065) Microsoft Internet Explorer Permission Validation II Privilege Escalation (3003057)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-6350

[Update Details](#)

Recommendation is updated

#### **17389 - (MS14-071) Vulnerability in Windows Audio Service Could Allow Elevation of Privilege (3005607)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-6322

[Update Details](#)

Recommendation is updated

#### **17390 - (MS14-071) Microsoft Windows Audio Services Privilege Escalation (3005607)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-6322

[Update Details](#)

Recommendation is updated

#### **17497 - (MS14-080) Microsoft Internet Explorer ASLR Security Bypass (3008923)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2014-6368

[Update Details](#)

Recommendation is updated

#### **17603 - (MS15-008) Vulnerabilities in Windows Kernel Mode Drivers Could Allow Elevation of Privilege (3019215)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0011

[Update Details](#)

Recommendation is updated

#### **17605 - (MS15-008) Microsoft Windows WebDAV Privilege Escalation (3019215)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-0011

[Update Details](#)

Recommendation is updated

---

### **18284 - (MS15-043) Microsoft Internet Explorer VBScript ASLR Security Bypass I (3049563)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1684

#### Update Details

Recommendation is updated

### **18285 - (MS15-043) Microsoft Internet Explorer ASLR Security Bypass (3049563)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1685

#### Update Details

Recommendation is updated

### **18286 - (MS15-043) Microsoft Internet Explorer VBScript ASLR Security Bypass II (3049563)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1686

#### Update Details

Recommendation is updated

### **18291 - (MS15-043) Microsoft Internet Explorer Clipboard Information Disclosure (3049563)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1692

#### Update Details

Recommendation is updated

### **18428 - (MS15-056) Microsoft Internet Explorer History Information Disclosure (3058515)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1765

#### Update Details

Recommendation is updated

### **18609 - (MS15-070) Microsoft Excel ASLR Bypass Information Disclosure (3072620)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2375

[Update Details](#)

Recommendation is updated

**18619 - (MS15-065) Microsoft Internet Explorer Information Disclosure I (3076321)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-1729

[Update Details](#)

Recommendation is updated

**18634 - (MS15-065) Microsoft Internet Explorer Filter Bypass Cross-Site Scripting I (3076321)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2398

[Update Details](#)

Recommendation is updated

**18642 - (MS15-065) Microsoft Internet Explorer Information Disclosure III (3076321)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2410

[Update Details](#)

Recommendation is updated

**18644 - (MS15-065) Microsoft Internet Explorer Information Disclosure IV (3076321)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2412

[Update Details](#)

Recommendation is updated

**18645 - (MS15-065) Microsoft Internet Explorer Information Disclosure V (3076321)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-2413

[Update Details](#)

Recommendation is updated

**18646 - (MS15-065) Microsoft Internet Explorer Information Disclosure VI (3076321)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-2414

[Update Details](#)

Recommendation is updated

**18648 - (MS15-065) Microsoft Internet Explorer ASLR Security Bypass (3076321)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-2421

[Update Details](#)

Recommendation is updated

**18653 - (MS15-065) Microsoft Internet Explorer Information Disclosure II (3076321)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-2402

[Update Details](#)

Recommendation is updated

**18761 - (MS15-079) Microsoft Internet Explorer Unsafe Command Line Parameter Information Disclosure (3082442)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-2423

[Update Details](#)

Recommendation is updated

**18772 - (MS15-079) Microsoft Internet Explorer ASLR Security Bypass I (3082442)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-2445

[Update Details](#)

Recommendation is updated

**18773 - (MS15-079) Microsoft Internet Explorer ASLR Security Bypass II (3082442)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2449

[Update Details](#)

Recommendation is updated

**18794 - (MS15-080) Microsoft Windows CSRSS Privilege Escalation (3078662)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2453

[Update Details](#)

Recommendation is updated

**18804 - (MS15-091) Microsoft Edge ASLR Bypass Security Bypass (3084525)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2449

[Update Details](#)

Recommendation is updated

**18817 - (MS15-088) Unsafe Command Line Parameter Passing Could Allow Information Disclosure (3082458)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2423

[Update Details](#)

Recommendation is updated

**18823 - (MS15-081) Microsoft Office Command Line Parameter Unsafe Passing Information Disclosure (3080790)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2423

[Update Details](#)

Recommendation is updated

**18830 - (MS15-088) Microsoft Windows Command Line Parameter Unsafe Passing Information Disclosure (3082458)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2423

[Update Details](#)

Recommendation is updated

**18934 - (MS15-094) Microsoft Internet Explorer Permissions Privilege Escalation (3089548)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2489

[Update Details](#)

Recommendation is updated

**18975 - (MS15-098) Microsoft Windows Journal Denial of Service (3089669)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2516

[Update Details](#)

Recommendation is updated

**19074 - (MS15-107) Microsoft Edge Filter Cross-Site Scripting (3096448)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6058

[Update Details](#)

Recommendation is updated

**19085 - (MS15-110) Microsoft SharePoint Information Disclosure (3089664)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-2556

[Update Details](#)

Recommendation is updated



### **19087 - (MS15-106) Microsoft Internet Explorer II Information Disclosure (3096441)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6046

#### Update Details

Recommendation is updated

### **19092 - (MS15-106) Microsoft Internet Explorer III Privilege Escalation (3096441)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6051

#### Update Details

Recommendation is updated

### **19093 - (MS15-106) Microsoft Internet Explorer VBScript and Jscript ASLR Security Bypass (3096441)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6052

#### Update Details

Recommendation is updated

### **19097 - (MS15-106) Microsoft Internet Explorer Information Disclosure (3096441)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6059

#### Update Details

Recommendation is updated

### **19221 - (MS15-113) Microsoft Edge ASLR Security Bypass (3104519)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6088

#### Update Details

Recommendation is updated

### **19233 - (MS15-118) Security Updates in .NET Framework to Address Elevation of Privilege (3104507)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6096, CVE-2015-6099, CVE-2015-6115

[Update Details](#)

Recommendation is updated

**19234 - (MS15-118) Microsoft .NET Framework ASLR Security Bypass (3104507)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6115

[Update Details](#)

Recommendation is updated

**19235 - (MS15-118) Microsoft .NET Framework DTD Parsing Privilege Escalation I (3104507)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6096

[Update Details](#)

Recommendation is updated

**19236 - (MS15-118) Microsoft .NET Framework HTTP Request Privilege Escalation II (3104507)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6099

[Update Details](#)

Recommendation is updated

**19262 - (MS15-112) Microsoft Internet Explorer Information Disclosure (3104517)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6086

[Update Details](#)

Recommendation is updated

**19264 - (MS15-112) Microsoft Internet Explorer ASLR Security Bypass (3104517)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-6088

[Update Details](#)

Recommendation is updated

**19270 - (MS15-122) Microsoft Windows Kerberos Password Change Security Bypass (3105256)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-6095

[Update Details](#)

Recommendation is updated

**19271 - (MS15-122) Security Update for Kerberos to Address Security Feature Bypass (3105256)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-6095

[Update Details](#)

Recommendation is updated

**19272 - (MS15-123) Microsoft Skype For Business Server Input Validation Information Disclosure (3105872)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-6061

[Update Details](#)

Recommendation is updated

**19273 - (MS15-123) Security Update for Skype for Business and Lync to Address Information Disclosure (3105872)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-6061

[Update Details](#)

Recommendation is updated

**19358 - (MS15-124) Microsoft Internet Explorer XSS Filter Security Bypass I (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium  
CVE: CVE-2015-6138

[Update Details](#)

Recommendation is updated

**19364 - (MS15-124) Microsoft Internet Explorer XSS Filter Security Bypass II (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6144

[Update Details](#)

Recommendation is updated

**19377 - (MS15-124) Microsoft Internet Explorer Memory Content Information Disclosure (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6157

[Update Details](#)

Recommendation is updated

**19381 - (MS15-124) Microsoft Internet Explorer ASLR Security Bypass (3116180)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6161

[Update Details](#)

Recommendation is updated

**19419 - (MS15-129) Microsoft Silverlight Information Disclosure II (3106614)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6165

[Update Details](#)

Recommendation is updated

**19420 - (MS15-129) Microsoft Silverlight Information Disclosure I (3106614)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2015-6114

[Update Details](#)

Recommendation is updated

#### **19622 - (MS16-011) Microsoft Edge ASLR Security Bypass (3134225)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0080

[Update Details](#)

Recommendation is updated

#### **19623 - (MS16-011) Microsoft Edge HTTP Parsing Spoofing Information Disclosure (3134225)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0077

[Update Details](#)

Recommendation is updated

#### **19628 - (MS16-015) Microsoft SharePoint XSS Privilege Escalation (3134226)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0039

[Update Details](#)

Recommendation is updated

#### **19654 - (MS16-009) Microsoft Internet Explorer Hyperlink Object Information Disclosure (3134220)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0059

[Update Details](#)

Recommendation is updated

#### **20017 - (MS16-055) Microsoft Windows Graphics Information Disclosure I (3156754)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0168

[Update Details](#)

Recommendation is updated

### **20018 - (MS16-055) Microsoft Windows Graphics Information Disclosure II (3156754)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0169

#### Update Details

Recommendation is updated

### **20022 - (MS16-065) Microsoft .NET Framework Encryption TLS/SSL Information Disclosure (3156757)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0149

#### Update Details

Recommendation is updated

### **20023 - (MS16-065) Security Update for .NET Framework (3156757)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-0149

#### Update Details

Recommendation is updated

### **20261 - (MS16-088) Microsoft Office XLA File Handling Remote Code Execution (3170008)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3279

#### Update Details

Recommendation is updated

### **20290 - (MS16-084) Microsoft Internet Explorer Restricted Ports Security Bypass (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3245

#### Update Details

Recommendation is updated

### **20302 - (MS16-085) Microsoft Edge Scripting Engine Information Disclosure (3169999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3271

Update Details

Recommendation is updated

**20310 - (MS16-085) Microsoft Edge Security Bypass (3169999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3244

Update Details

Recommendation is updated

**20395 - (MS16-103) Security Update for ActiveSyncProvider (3182332)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3312

Update Details

Recommendation is updated

**20530 - (MS16-111) Security Update for Windows Kernel (3186973)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-2016-3305, CVE-2016-3306, CVE-2016-3371, CVE-2016-3372, CVE-2016-3373

Update Details

Recommendation is updated

**130599 - Debian Linux 8.0 DSA-3685-1 Update Is Not Installed**

Category: SSH Module -> NonIntrusive -> Debian Patches and Hotfixes

Risk Level: Medium

CVE: CVE-2016-7424

Update Details

Risk is updated

**18592 - (MS15-071) Vulnerability in NETLOGON Could Allow Spoofing (3068457)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2374

[Update Details](#)

Recommendation is updated

**18595 - (MS15-071) Microsoft Windows NETLOGON Spoofing Information Disclosure (3068457)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2374

[Update Details](#)

Recommendation is updated

**18945 - (MS15-099) Microsoft Office Sharepoint Cross Site Scripting Information Disclosure (3089664)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2522

[Update Details](#)

Recommendation is updated

**19107 - (MS15-110) Microsoft Office Web Apps Spoofing Cross-Site Scripting (3089664)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-6037

[Update Details](#)

Recommendation is updated

**19108 - (MS15-110) Microsoft SharePoint Security Bypass (3089664)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-6039

[Update Details](#)

Recommendation is updated

**19230 - (MS15-115) Microsoft Windows Kernel Permissions Validation Security Bypass (3105864)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-6113



[Update Details](#)

Recommendation is updated

**12336 - (MS11-054) Microsoft Windows Win32k Incorrect Parameter Privilege Escalation (2555917)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2011-1886

[Update Details](#)

Recommendation is updated

**18463 - (MS15-061) Microsoft Windows Kernel Information Disclosure (3057839)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-1719

[Update Details](#)

Recommendation is updated

**18471 - (MS15-061) Microsoft Windows Kernel Brush Object Use-After-Free Privilege Escalation (3057839)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-1726

[Update Details](#)

Recommendation is updated

**18472 - (MS15-061) Microsoft Windows Win32k Pool Buffer Overflow Privilege Escalation (3057839)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-1727

[Update Details](#)

Recommendation is updated

**18473 - (MS15-061) Microsoft Windows Win32k Memory Corruption Privilege Escalation (3057839)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-1768

[Update Details](#)

Recommendation is updated

#### **18600 - (MS15-073) Microsoft Windows Kernel I Information Disclosure (3070102)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2367

[Update Details](#)

Recommendation is updated

#### **18601 - (MS15-073) Microsoft Windows Kernel II Information Disclosure (3070102)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2381

[Update Details](#)

Recommendation is updated

#### **18602 - (MS15-073) Microsoft Windows Kernel III Information Disclosure (3070102)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2382

[Update Details](#)

Recommendation is updated

#### **18795 - (MS15-080) Microsoft Windows KMD Security Bypass (3078662)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2454

[Update Details](#)

Recommendation is updated

#### **18796 - (MS15-080) Microsoft Windows Shell Security Bypass (3078662)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2465

[Update Details](#)

Recommendation is updated

---

**18798 - (MS15-080) Microsoft Windows Kernel ASLR Security Bypass (3078662)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2433

Update Details

Recommendation is updated

**18818 - (MS15-089) Vulnerability in WebDAV Could Allow Information Disclosure (3076949)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2476

Update Details

Recommendation is updated

**18831 - (MS15-089) Microsoft Windows WebDAV Client Information Disclosure (3076949)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2476

Update Details

Recommendation is updated

**18971 - (MS15-097) Microsoft Windows Graphics Security Bypass (3089656)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2529

Update Details

Recommendation is updated

**19226 - (MS15-115) Microsoft Windows Kernel KASLR Information Disclosure I (3105864)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-6102

Update Details

Recommendation is updated

**19229 - (MS15-115) Microsoft Windows Kernel KASLR Information Disclosure II (3105864)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-6109

Update Details

Recommendation is updated

**19668 - (MS16-014) Microsoft Windows Kerberos Security Bypass (3134228)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0049

Update Details

Recommendation is updated

**20015 - (MS16-051) Microsoft Internet Explorer Information Disclosure (3155533)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0194

Update Details

Recommendation is updated

**20024 - (MS16-066) Microsoft Windows Hypervisor Code Integrity Security Bypass (3155451)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0181

Update Details

Recommendation is updated

**20025 - (MS16-066) Security Update for Virtual Secure Mode (3155451)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0181

Update Details

Recommendation is updated

**20037 - (MS16-062) Microsoft Windows Kernel Information Disclosure (3158222)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-0175

[Update Details](#)

Recommendation is updated

**20269 - (MS16-090) Microsoft Windows Kernel GDI Information Disclosure (3171481)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3251

[Update Details](#)

Recommendation is updated

**20275 - (MS16-092) Security Update for Windows Kernel (3171910)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3258, CVE-2016-3272

[Update Details](#)

Recommendation is updated

**20276 - (MS16-092) Microsoft Windows Kernel Information Disclosure (3171910)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3272

[Update Details](#)

Recommendation is updated

**20278 - (MS16-094) Microsoft Windows Secure Boot Security Bypass (3177404)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3287

[Update Details](#)

Recommendation is updated

**20281 - (MS16-084) Microsoft Internet Explorer Browser Spoofing II (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3276

[Update Details](#)

Recommendation is updated

**20282 - (MS16-084) Microsoft Internet Explorer Browser Spoofing I (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3274

[Update Details](#)

Recommendation is updated

**20283 - (MS16-084) Microsoft Internet Explorer Browser Cross-Site Scripting (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3273

[Update Details](#)

Recommendation is updated

**20284 - (MS16-084) Microsoft Internet Explorer Information Disclosure II (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3277

[Update Details](#)

Recommendation is updated

**20285 - (MS16-084) Microsoft Internet Explorer Information Disclosure I (3169991)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3261

[Update Details](#)

Recommendation is updated

**20297 - (MS16-094) Security Update for Secure Boot (3177404)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3287

[Update Details](#)

Recommendation is updated

#### **20299 - (MS16-085) Microsoft Edge Browser Spoofing II (3169999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3276

[Update Details](#)

Recommendation is updated

#### **20300 - (MS16-085) Microsoft Edge Browser Spoofing I (3169999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3274

[Update Details](#)

Recommendation is updated

#### **20301 - (MS16-085) Microsoft Edge Browser Information Disclosure (3169999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3273

[Update Details](#)

Recommendation is updated

#### **20308 - (MS16-085) Microsoft Edge Memory Corruption Remote Code Execution III (3169999)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3277

[Update Details](#)

Recommendation is updated

#### **20311 - (MS16-089) Security Update for Windows Secure Kernel Mode (3170050)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3256

[Update Details](#)

Recommendation is updated

**20312 - (MS16-089) Microsoft Windows Secure Kernel Information Disclosure (3170050)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3256

Update Details

Recommendation is updated

**18273 - (MS15-052) Vulnerability in Windows Kernel Could Allow Security Feature Bypass (3050514)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-1674

Update Details

Recommendation is updated

**18299 - (MS15-052) Microsoft Windows Kernel Security Bypass (3050514)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-1674

Update Details

Recommendation is updated

**18926 - (MS15-105) Vulnerability in Windows Hyper-V Could Allow Security Feature Bypass (3091287)**

Category: Windows Host Assessment -> Patches Only  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2534

Update Details

Recommendation is updated

**18927 - (MS15-105) Microsoft Windows Hyper-V Security Bypass (3091287)**

Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2015-2534

Update Details

Recommendation is updated

**20277 - (MS16-092) Microsoft Windows File System Security Feature Security Bypass (3171910)**



Category: Windows Host Assessment -> Patches and Hotfixes  
(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Low

CVE: CVE-2016-3258

#### Update Details

Recommendation 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.

This email may contain confidential and privileged material for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient please contact the sender and delete all copies.

Copyright 2016 McAfee, Inc.

McAfee is a registered trademark of McAfee, Inc. and/or its affiliates