

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

20069 - (APSB16-14) Vulnerabilities In Adobe Reader And Acrobat

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

Risk Level: High

CVE: CVE-2016-1037, CVE-2016-1038, CVE-2016-1039, CVE-2016-1040, CVE-2016-1041, CVE-2016-1042, CVE-2016-1043, CVE-2016-1044, CVE-2016-1045, CVE-2016-1046, CVE-2016-1047, CVE-2016-1048, CVE-2016-1049, CVE-2016-1050, CVE-2016-1051, CVE-2016-1052, CVE-2016-1053, CVE-2016-1054, CVE-2016-1055, CVE-2016-1056, CVE-2016-1057, CVE-2016-1058, CVE-2016-1059, CVE-2016-1060, CVE-2016-1061, CVE-2016-1062, CVE-2016-1063, CVE-2016-1064, CVE-2016-1065, CVE-2016-1066, CVE-2016-1067, CVE-2016-1068, CVE-2016-1069, CVE-2016-1070, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1075, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1079, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1087, CVE-2016-1088, CVE-2016-1090, CVE-2016-1092, CVE-2016-1093, CVE-2016-1094, CVE-2016-1095, CVE-2016-1112, CVE-2016-1116, CVE-2016-1117, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1121, CVE-2016-1122, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4091, CVE-2016-4092, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4102, CVE-2016-4103, CVE-2016-4104, CVE-2016-4105, CVE-2016-4106, CVE-2016-4107

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 multiple memory corruption issues and due to an uncontrolled search path element. Successful exploitation could allow an attacker to remotely execute arbitrary code, bypass security restrictions or retrieve sensitive data.

The update provided by Adobe bulletin APSB16-14 resolves these issues. The target system appears to be missing this update.

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

Description

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

Observation

Microsoft Internet Explorer is a popular internet 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 escalate privileges, obtain sensitive information, bypass security measures or execute remote code.

Microsoft has provided MS16-051 to address these issues. The host appears to be missing this patch.

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

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 VBScript engine renders when handling objects in memory in Internet Explorer. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

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

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 VBScript engine renders when handling objects in memory in Internet Explorer. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

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

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

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

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 way Windows GDI component and Windows Imaging Component handle objects in memory. Successful exploitation by a remote attacker could result in disclosure of information or execution of remote code.

Microsoft has provided MS16-055 to address these issues. The host appears to be missing this patch.

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

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 in Microsoft Edge. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

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

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

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

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 in Microsoft Edge. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

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

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

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

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.

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

Description

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

Observation

A vulnerability in some versions of Microsoft Office 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.

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

Description

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

Observation

Microsoft Windows is a popular operating system.

A remote code execution vulnerability is present in some versions of Microsoft Windows. The flaw occurs in Microsoft Windows if a specially crafted Journal file is opened in Windows Journal. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

Microsoft has provided MS16-056 to address this issue. The host appears to be missing this patch.

20053 - (MS16-053) Microsoft VBScript Memory Corruption Remote Code Execution II (3156764)

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

Risk Level: High

CVE: CVE-2016-0189

Description

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

Observation

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

The flaw occurs in the way that the VBScript engine renders when handling objects in memory in Internet Explorer. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

20054 - (MS16-053) Microsoft VBScript Memory Corruption Remote Code Execution I (3156764)

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

Risk Level: High

CVE: CVE-2016-0187

Description

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

Observation

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

The flaw occurs in the way that the VBScript engine renders when handling objects in memory in Internet Explorer. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

20055 - (MS16-053) Security Update for JScript and VBScript (3156764)

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

Risk Level: High

CVE: CVE-2016-0187, CVE-2016-0189

Description

Multiple remote code execution vulnerabilities exists in some versions of Microsoft Windows.

Observation

Microsoft Windows is a popular operating system.

Multiple remote code execution vulnerabilities exists in some versions of Microsoft Windows. The flaws lie in how the JScript and VBScript engines render, when handling objects in memory in Internet Explorer. Successful exploitation by a remote attacker could result in the execution of arbitrary code.

Microsoft has provided MS16-053 to address this issue. The host appears to be missing this patch.

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

Description

A remote code execution vulnerability exists in some versions of Microsoft Windows.

Observation

Microsoft Windows is a popular operating system.

A remote code execution vulnerability exists in some versions of Microsoft Windows. The flaw lies in how the Windows Shell component handles objects in memory. Successful exploitation could allow an attacker to execute remote code.

Microsoft has provided MS16-057 to address this issue. The host appears to be missing this patch.

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

Description

Multiple vulnerabilities are present in some versions of Microsoft Office.

Observation

Microsoft Office is a popular office suite.

Multiple vulnerabilities are present in some versions of Microsoft Office. The flaws are related with bad object handling in memory and with how Windows font library handles specially crafted embedded fonts. Successful exploitation could allow an attacker to remotely execute arbitrary code.

Microsoft has provided MS16-054 to address these issues. The host appears to be missing this patch.

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

Description

Multiple vulnerabilities are present in some versions of Microsoft Edge.

Observation

Microsoft Edge is a new 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 remotely execute arbitrary code.

Microsoft has provided MS16-052 to address these issues. The host appears to be missing this patch.

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

Description

Multiple vulnerabilities are present in some versions of Microsoft Office.

Observation

Microsoft Office is a popular office suite.

Multiple vulnerabilities are present in some versions of Microsoft Office. The flaws are related with bad object handling in memory and with how Windows font library handles specially crafted embedded fonts. Successful exploitation could allow an attacker to remotely execute arbitrary code.

Microsoft has provided MS16-054 to address these issues. The host appears to be missing this patch.

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

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 is due to the way the Windows Kernel handles Remote Procedure Calls. Successful exploitation could allow an attacker to escalate privileges.

Microsoft has provided MS16-061 to address this issue. The host appears to be missing this patch.

20009 - (MS16-058) Microsoft Windows IIS DLL Loading Remote Code Execution (3141083)

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

Risk Level: High

CVE: CVE-2016-0152

Description

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

Observation

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

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

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

Description

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

Observation

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

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

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

Description

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

Observation

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

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

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

Description

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

Observation

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

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

20047 - (MS16-059) Security Update for Windows Media Center (3150220)

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

Risk Level: High

CVE: CVE-2016-0185

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

Microsoft has provided MS16-059 to address this issue. The host appears to be missing this patch.

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

Description

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

Observation

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

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

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

Description

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

Observation

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

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

20007 - (MS16-058) Security Update for Windows IIS (3141083)

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

Risk Level: Medium

CVE: CVE-2016-0152

Description

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

Observation

Microsoft Windows is an industry standard operating system.

A remote code execution vulnerability is present in some versions of Microsoft Windows. The flaw is due to the way Windows validate input before loading certain libraries. Successful exploitation could allow an attacker to execute remote code. The exploit requires the attacker to have valid credentials to the vulnerable system.

Microsoft has provided MS16-058 to address this issue. The host appears to be missing this patch.

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

Description

An information disclosure vulnerability exist in some versions of Microsoft Windows .NET Framework.

Observation

Microsoft .NET framework is a runtime and software framework for the Windows operating system.

An information disclosure vulnerability exist in some versions of Microsoft Windows .NET Framework. The flaw is due to how Microsoft .NET Framework implements TLS/SSL protocol. Successful exploitation could allow a remote attacker to disclose information.

Microsoft has provided MS16-065 to address this issue. The host appears to be missing this patch.

20042 - (MS16-062) Security Update for Windows Kernel-Mode Drivers (3158222)

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

Risk Level: Medium

CVE: CVE-2016-0171, CVE-2016-0173, CVE-2016-0174, CVE-2016-0175, CVE-2016-0176, CVE-2016-0196, CVE-2016-0197

Description

Multiple privilege escalation vulnerabilities are present in some versions of Microsoft Windows.

Observation

Microsoft Windows is a popular operating system.

Multiple privilege escalation vulnerabilities are present in some versions of Microsoft Windows. The flaws lie in how objects are handled in memory by the Windows Kernel-mode driver and the DirectX Graphics kernel subsystem. Successful exploitation by an attacker could result in an elevation of its privilege leading to arbitrary code execution, information disclosure or creation of new user accounts with full user rights. Exploitation of this vulnerability requires the malicious user to log on to the target system.

Microsoft has provided MS16-062 to address this issue. The host appears to be missing this patch.

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: Medium

CVE: CVE-2016-0178

Description

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

Observation

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

The flaw lies in the Remote Procedure Call component. Successful exploitation could allow a local user to gain elevated privileges.

20012 - (MS16-051) Microsoft Internet Explorer Security Bypass (3155533)

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

Risk Level: Medium

CVE: CVE-2016-0188

Description

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

Observation

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

The flaw occurs in the User Mode Code Integrity (UMCI) component of Device Guard, when it improperly validates code integrity. Successful exploitation could allow a remote attacker to bypass intended access restrictions.

20015 - (MS16-051) Microsoft Internet Explorer Information Disclosure (3155533)

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

Risk Level: Medium

CVE: CVE-2016-0194

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 Internet Explorer does not properly handle files, which could allow an attacker to disclose the contents of arbitrary files on the user's computer. Successful exploitation by a remote attacker could result in the disclosure of sensitive information.

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

Description

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

Observation

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

The flaw lies in the Graphics component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

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

Description

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

Observation

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

The flaw lies in the Graphics component. Successful exploitation by a remote attacker could result in the disclosure of sensitive information. The exploit requires the user to open a vulnerable website, email or document.

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

Description

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

Observation

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

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

20024 - (MS16-066) Microsoft Windows Hypervisor Code Integrity Security Bypass (3155451)

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

Risk Level: Medium

CVE: CVE-2016-0181

Description

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

Observation

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

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

20025 - (MS16-066) Security Update for Virtual Secure Mode (3155451)

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

Risk Level: Medium

CVE: CVE-2016-0181

Description

A vulnerability is present in some versions of Microsoft Windows.

Observation

Microsoft Windows is a popular operating system.

A vulnerability is present in some versions of Microsoft Windows. The flaw lies in the Hypervisor Code Integrity feature. Successful exploitation by a remote attacker could result in the bypass of code integrity protections of the operating system. Exploitation requires a malicious user to execute a specially crafted application.

Microsoft has provided MS16-066 to address this issue. The host appears to be missing this patch.

20030 - (MS16-054) Microsoft Office Memory Corruption Remote Code Execution I (3155544)

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

Risk Level: Medium

CVE: CVE-2016-0126

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.

20031 - (MS16-054) Microsoft Office Memory Corruption Remote Code Execution II (3155544)

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

Risk Level: Medium

CVE: CVE-2016-0140

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.

20034 - (MS16-067) Security Update for Volume Manager Driver (3155784)

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

Risk Level: Medium

CVE: CVE-2016-0190

Description

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

Observation

Microsoft Windows is a popular operating system.

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

Microsoft has provided MS16-067 to address this issue. The host appears to be missing this patch.

20035 - (MS16-059) Microsoft Windows Media Center Mcl file Privilege Escalation (3150220)

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

Risk Level: Medium

CVE: CVE-2016-0185

Description

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

Observation

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

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

20036 - (MS16-062) Microsoft Windows Kernel DirectX Subsystem Privilege Escalation I (3158222)

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

Risk Level: Medium

CVE: CVE-2016-0176

Description

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

Observation

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

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

20037 - (MS16-062) Microsoft Windows Kernel Information Disclosure (3158222)

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

Risk Level: Medium

CVE: CVE-2016-0175

Description

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

Observation

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

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

20038 - (MS16-062) Microsoft Windows Kernel Privilege Escalation IV (3158222)

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

Risk Level: Medium

CVE: CVE-2016-0174

Description

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

Observation

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

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

20039 - (MS16-062) Microsoft Windows Kernel Privilege Escalation III (3158222)

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

Risk Level: Medium

CVE: CVE-2016-0173

Description

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

Observation

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

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

20041 - (MS16-062) Microsoft Windows Kernel Privilege Escalation I (3158222)

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

Risk Level: Medium

CVE: CVE-2016-0171

Description

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

Observation

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

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

20043 - (MS16-060) Microsoft Windows Kernel Symbolic Links Privilege Escalation (3154846)

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

Risk Level: Medium

CVE: CVE-2016-0180

Description

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

Observation

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

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

20044 - (MS16-067) Microsoft Windows USB Driver RDP Drive Redirection Information Disclosure (3155784)

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

Risk Level: Medium
CVE: CVE-2016-0190

Description

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

Observation

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

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

20045 - (MS16-062) Microsoft Windows Kernel DirectX Subsystem Privilege Escalation II (3158222)

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

Risk Level: Medium
CVE: CVE-2016-0197

Description

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

Observation

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

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

20048 - (MS16-060) Security Update for Windows Kernel (3154846)

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

Risk Level: Medium
CVE: CVE-2016-0180

Description

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

Observation

Microsoft Windows is a popular operating system.

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

Microsoft has provided MS16-060 to address this issue. The host appears to be missing this patch.

20050 - (MS16-062) Microsoft Windows Kernel Privilege Escalation V (3158222)

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

Risk Level: Medium
CVE: CVE-2016-0196

Description

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

Observation

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

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

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

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

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

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

19991 - Mozilla Firefox Multiple Vulnerabilities Prior To 46

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

Risk Level: High

CVE: CVE-2016-2804, CVE-2016-2806, CVE-2016-2807, CVE-2016-2808, CVE-2016-2809, CVE-2016-2811, CVE-2016-2812, CVE-2016-2814, CVE-2016-2816, CVE-2016-2817, CVE-2016-2820

[Update Details](#)

Risk is updated

19992 - Mozilla Firefox Multiple Vulnerabilities Prior To 46

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: High

CVE: CVE-2016-2804, CVE-2016-2806, CVE-2016-2807, CVE-2016-2808, CVE-2016-2809, CVE-2016-2811, CVE-2016-2812, CVE-2016-2814, CVE-2016-2816, CVE-2016-2817, CVE-2016-2820

[Update Details](#)

Risk is updated

88769 - Slackware Linux 14.0, 14.1 SSA:2016-124-01 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176

[Update Details](#)

Risk is updated

130479 - Debian Linux 8.0 DSA-3566-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176

[Update Details](#)

Risk is updated

130482 - Debian Linux 8.0 DSA-3562-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-0857, CVE-2015-0858

[Update Details](#)

Risk is updated

130486 - Debian Linux 8.0 DSA-3567-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-4422

[Update Details](#)

Risk is updated

144558 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1138-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-1601

[Update Details](#)

Risk is updated

144567 - SuSE SLES 12 SP1, SLED 12 SP1 SUSE-SU-2016:1233-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109

[Update Details](#)

Risk is updated

144574 - SuSE SLES 12, SLED 12 SUSE-SU-2016:1228-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109

[Update Details](#)

Risk is updated

144577 - SuSE Linux 13.2 openSUSE-SU-2016:1238-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109

[Update Details](#)

Risk is updated

144579 - SuSE Linux 13.1 openSUSE-SU-2016:1240-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109

[Update Details](#)

Risk is updated

144580 - SuSE Linux 11.4 openSUSE-SU-2016:1237-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109

[Update Details](#)

Risk is updated

170672 - Amazon Linux AMI ALAS-2016-695 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109

[Update Details](#)

Risk is updated

181933 - FreeBSD OpenSSL Multiple Vulnerabilities (01d729ca-1143-11e6-b55e-b499baebfeaf)

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176

[Update Details](#)

Risk is updated

185256 - Ubuntu Linux 12.04, 14.04, 15.10, 16.04 USN-2959-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109

[Update Details](#)

Risk is updated

185257 - Ubuntu Linux 14.04 USN-2961-1 Update Is Not Installed

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

Risk Level: High
CVE: CVE-2013-7455

Update Details

Risk is updated

190587 - Fedora Linux 23 FEDORA-2016-05c567df1a Update Is Not Installed

Category: SSH Module -> NonIntrusive -> Fedora Patches and Hotfixes
Risk Level: High
CVE: CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108

Update Details

Risk 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

5810 - (MS08-021) Microsoft GDI Heap Overflow Vulnerability (948590)

Category: Windows Host Assessment -> Patches and Hotfixes
(CATEGORY REQUIRES CREDENTIALS)
Risk Level: High
CVE: CVE-2008-1083, CVE-2008-1087

[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

6273 - (MS08-071) Microsoft GDI Heap Overflow Vulnerability (956802)

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

Risk Level: High

CVE: CVE-2008-3465

[Update Details](#)

Recommendation is updated

6274 - (MS08-071) Microsoft GDI Integer Overflow Vulnerability (956802)

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

Risk Level: High

CVE: CVE-2008-2249

[Update Details](#)

Recommendation is updated

7098 - (MS09-045) Microsoft Windows Jscript Remote Code Execution Vulnerability (971961)

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

Risk Level: High

CVE: CVE-2009-1920

[Update Details](#)

Recommendation is updated

7172 - (MS09-045) Vulnerability In JScript Scripting Engine Could Allow Remote Code Execution (971961)

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

Risk Level: High

CVE: CVE-2009-1920

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

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

8297 - (MS08-071) Vulnerabilities In GDI Could Allow Remote Code Execution (956802)

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

Risk Level: High

CVE: CVE-2008-2249, CVE-2008-3465

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

8546 - (MS10-022) Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981169)

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

Risk Level: High

CVE: CVE-2010-0483

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

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

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

11767 - (MS11-031) Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2514666)

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

Risk Level: High

CVE: CVE-2011-0663

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

11827 - (MS11-031) Microsoft Scripting Engines Memory Reallocation Remote Code Execution (2514666)

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

Risk Level: High

CVE: CVE-2011-0663

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

12616 - (MS11-072) Microsoft Excel Conditional Expression Parsing Remote Code Execution (2587505)

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

Risk Level: High

CVE: CVE-2011-1989

Update Details

Recommendation is updated

12617 - (MS11-072) Microsoft Excel Heap Corruption Remote Code Execution (2587505)

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

Risk Level: High

CVE: CVE-2011-1988

Update Details

Recommendation is updated

12618 - (MS11-072) Microsoft Excel Out of Bounds Array Indexing Remote Code Execution (2587505)

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

Risk Level: High

CVE: CVE-2011-1987

Update Details

Recommendation is updated

12619 - (MS11-072) Microsoft Excel Out of Bounds Array Indexing Remote Code Execution II (2587505)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1990

[Update Details](#)

Recommendation is updated

12620 - (MS11-072) Microsoft Excel Use after Free WriteAV Remote Code Execution (2587505)

Category: Windows Host Assessment -> Patches and Hotfixes

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1986

[Update Details](#)

Recommendation is updated

12627 - (MS11-072) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2587505)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2011-1986, CVE-2011-1987, CVE-2011-1988, CVE-2011-1989, CVE-2011-1990

[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

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

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

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

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

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

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

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

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

15702 - (MS13-085) Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2885080)

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

Risk Level: High

CVE: CVE-2013-3889, CVE-2013-3890

Update Details

Recommendation is updated

15703 - (MS13-085) Microsoft Excel Memory Corruption Remote Code Execution I (2885080)

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

Risk Level: High

CVE: CVE-2013-3889

Update Details

Recommendation is updated

15719 - (MS13-085) Microsoft Excel Memory Corruption Remote Code Execution I (2885080)

Category: SSH Module -> NonIntrusive -> Mac OS X Patches and Hotfixes

Risk Level: High

CVE: CVE-2013-3889

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

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

15780 - EATON VURemote Denial of Service

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

Risk Level: High
CVE: CVE-MAP-NOMATCH

Update Details

Recommendation is updated

15909 - (MS13-089) Microsoft Windows Graphics Device Interface Remote Code Execution (2876331)

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

Risk Level: High
CVE: CVE-2013-3940

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

15912 - (MS13-089) Vulnerability in Windows Graphics Device Interface Could Allow Remote Code Execution (2876331)

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

Risk Level: High
CVE: CVE-2013-3940

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

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

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

16258 - Eaton Network Shutdown Module Pi3Web WebServer Denial of Service

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA

Risk Level: High

CVE: CVE-MAP-NOMATCH

[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

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

16445 - Delta Electronics WPLSoft DVPSimulator.exe Buffer Overflow Remote Code Execution

Category: General Vulnerability Assessment -> Intrusive -> SCADA

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

16461 - (MS12-056) Microsoft Windows Jscript and VBScript Remote Code Execution (2706045)

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

Risk Level: High

CVE: CVE-2012-2523

[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

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

17353 - Emerson ROCLINK 800 apro2.dll ActiveX Control Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

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

17484 - (MS14-084) Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3016711)

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

Risk Level: High

CVE: CVE-2014-6363

[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

17495 - (MS14-084) Microsoft VBScript Memory Corruption Remote Code Execution (3016711)

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

Risk Level: High

CVE: CVE-2014-6363

[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

17975 - (MS15-019) Microsoft Windows VBScript Scripting Engine Remote Code Execution (3040297)

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

Risk Level: High
CVE: CVE-2015-0032

[Update Details](#)

Recommendation is updated

17983 - (MS15-019) Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3040297)

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

Risk Level: High
CVE: CVE-2015-0032

[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

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

18063 - Cogent DataHub Web Server Gamma Injection Remote Code Execution

Category: General Vulnerability Assessment -> Intrusive -> SCADA

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

18064 - Cogent DataHub Web Server Gamma Injection Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[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

18160 - (MS15-035) Vulnerability in Microsoft Graphics Component Could Allow Remote Code (3046306)

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

Risk Level: High

CVE: CVE-2015-1645

Update Details

Recommendation is updated

18161 - (MS15-035) Microsoft Windows EMF Processing Remote Code Execution (3046306)

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

Risk Level: High

CVE: CVE-2015-1645

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

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

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

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

18622 - (MS15-066) Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3072604)

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

Risk Level: High

CVE: CVE-2015-2372

[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

18625 - (MS15-066) Microsoft VBScript Memory Corruption Remote Code Execution (3072604)

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

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

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

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

18982 - (MS15-100) Microsoft Windows Media Center Remote Code Execution (3087918)

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

Risk Level: High

CVE: CVE-2015-2509

Update Details

Recommendation is updated

18986 - (MS15-100) Vulnerability in Windows Media Center Could Allow Remote Code Execution (3087918)

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

Risk Level: High

CVE: CVE-2015-2509

Update Details

Recommendation is updated

19068 - (MS15-108) Microsoft Scripting Engine Memory Corruption Remote Code Execution I (3089659)

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

Risk Level: High

CVE: CVE-2015-2482

Update Details

Recommendation is updated

19069 - (MS15-108) Microsoft Scripting Engine Memory Corruption Remote Code Execution II (3089659)

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

Risk Level: High

CVE: CVE-2015-6055

Update Details

Recommendation is updated

19076 - (MS15-108) Security Update for JScript and VBScript to Address Remote Code Execution (3089659)

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

Risk Level: High

CVE: CVE-2015-2482, CVE-2015-6052, CVE-2015-6055, CVE-2015-6059

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

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

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

19350 - (MS15-134) Security Update for Windows Media Center to Address Remote Code Execution (3108669)

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

Risk Level: High

CVE: CVE-2015-6127, CVE-2015-6131

Update Details

Recommendation is updated

19352 - (MS15-134) Microsoft Windows Media Center Library Parsing Remote Code Execution (3108669)

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

Risk Level: High

CVE: CVE-2015-6131

Update Details

Recommendation is updated

19525 - (MS16-003) Microsoft Jscript and VBScript Engine Memory Corruption Remote Code Execution (3125540)

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

19532 - (MS16-003) Cumulative Security Update for JScript and VBScript to Address Remote Code Execution (3125540)

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

Risk Level: High

CVE: CVE-2016-0002

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

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

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

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

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

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

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

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

130477 - Debian Linux 8.0 DSA-3563-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8868

[Update Details](#)

Risk is updated

190539 - Fedora Linux 22 FEDORA-2016-3c4e438fc8 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8868

[Update Details](#)

Risk is updated

190567 - Fedora Linux 23 FEDORA-2016-c848d48286 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8868

[Update Details](#)

Risk 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

5809 - (MS08-021) Microsoft GDI stack Overflow Vulnerability (948590)

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

Risk Level: High

CVE: CVE-2008-1083, CVE-2008-1087

[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 WordRTF 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

7645 - (MS08-021) Vulnerabilities In GDI Could Allow Remote Code Execution (948590)

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

Risk Level: High

CVE: CVE-2008-1083, CVE-2008-1087

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

8872 - Callisto PhotoParade Player PhPInfo ActiveX Control Buffer Overflow Vulnerability

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

Risk Level: High

CVE: CVE-2007-1688

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

14026 - (MS12-056) Vulnerability In JScript and VBScript Engines Could Allow Remote Code Execution (2706045)

Category: Windows Host Assessment -> Patches Only

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2012-2523

[Update Details](#)

Recommendation is updated

14154 - EMC AutoStart Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

14158 - EMC AlphaStor Remote Code Execution

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: High

CVE: CVE-MAP-NOMATCH

[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

14260 - CYME Power Engineering ChartFX Client Server ActiveX Control Array Indexing Remote Code Execution

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

Risk Level: High

CVE: CVE-MAP-NOMATCH

[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

19705 - SAP 3D Visual Enterprise Viewer SketchUp Document Multiple Use-After-Free Remote Code Execution Vulnerabilities

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-MAP-NOMATCH

[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

8535 - (MS10-022) Microsoft VBScript Help Keypress Vulnerability (981169)

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

Risk Level: High

CVE: CVE-2010-0483

[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

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

13182 - CoCSoft Stream Down Response Buffer Overflow Remote Code Execution

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

Risk Level: High

CVE: CVE-2011-5052

[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

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

15423 - DotNetNuke DNNArticle Module "categoryid" SQL Injection Vulnerability

Category: General Vulnerability Assessment -> Intrusive -> Web Server

Risk Level: High

CVE: CVE-2013-5117

Update Details

Recommendation is updated Documentation 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

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

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

16600 - (MS14-023) Vulnerability in Microsoft Office Could Allow Remote Code Execution (2961037)

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

Risk Level: High

CVE: CVE-2014-1756, CVE-2014-1808

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

16998 - (MS14-045) Microsoft Windows Font Double-Fetch Privilege Escalation (2984615)

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

Risk Level: High

CVE: CVE-2014-1819

Update Details

Recommendation is updated

17000 - (MS14-045) Microsoft Windows Win32k Privilege Escalation (2984615)

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

Risk Level: High

CVE: CVE-2014-0318

Update Details

Recommendation is updated

17011 - (MS14-045) Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation of Privilege (2984615)

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

Risk Level: High

CVE: CVE-2014-0318, CVE-2014-1819, CVE-2014-4064

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

18593 - (MS15-072) Vulnerability in Windows Graphics Component Could Allow Elevation of Privilege (3069392)

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

Risk Level: High

CVE: CVE-2015-2364

Update Details

Recommendation is updated

18594 - (MS15-072) Microsoft Windows Graphics Component Privilege Escalation (3069392)

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

Risk Level: High

CVE: CVE-2015-2364

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

19708 - Netgear Management System NMS300 Multiple Vulnerabilities

Category: General Vulnerability Assessment -> Intrusive -> Web Server

Risk Level: High

CVE: CVE-2016-1524, CVE-2016-1525

[Update Details](#)

Recommendation is updated

19716 - Wireshark Multiple Vulnerabilities Prior To 1.12.10

Category: Windows Host Assessment -> Miscellaneous

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: High

CVE: CVE-2016-2521, CVE-2016-2523, CVE-2016-2530, CVE-2016-2531, CVE-2016-2532, CVE-2016-4417, CVE-2016-4418, CVE-2016-4421

[Update Details](#)

CVE is updated

19717 - Wireshark Multiple Vulnerabilities Prior To 2.0.2

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

Risk Level: High

CVE: CVE-2016-2521, CVE-2016-2522, CVE-2016-2523, CVE-2016-2524, CVE-2016-2525, CVE-2016-2526, CVE-2016-2527, CVE-2016-2528, CVE-2016-2529, CVE-2016-2530, CVE-2016-2531, CVE-2016-2532, CVE-2016-4415, CVE-2016-4416, CVE-2016-4417, CVE-2016-4418, CVE-2016-4419, CVE-2016-4420, CVE-2016-4421

[Update Details](#)

CVE 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

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

88772 - Slackware Linux 14.0, 14.1 SSA:2016-120-02 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3074

[Update Details](#)

Risk is updated

130467 - Debian Linux 7.0, 8.0 DSA-3550-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8325

[Update Details](#)

Risk is updated

130471 - Debian Linux 7.0, 8.0 DSA-3556-1 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3074

[Update Details](#)

Risk is updated

181935 - FreeBSD php Multiple Vulnerabilities (5764c634-10d2-11e6-94fa-002590263bf5)

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

Risk Level: High

CVE: CVE-2016-3074

[Update Details](#)

Risk is updated

190438 - Fedora Linux 23 FEDORA-2016-02ed08bf15 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3134, CVE-2016-3135, CVE-2016-3156

[Update Details](#)

Risk is updated

190465 - Fedora Linux 22 FEDORA-2016-3a57b19360 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3134, CVE-2016-3135, CVE-2016-3156

[Update Details](#)

Risk is updated

190562 - Fedora Linux 23 FEDORA-2016-7f5004093e Update Is Not Installed

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

Risk Level: High

CVE: CVE-2015-8325

[Update Details](#)

Risk is updated

190581 - Fedora Linux 23 FEDORA-2016-5f91f43826 Update Is Not Installed

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

Risk Level: High

CVE: CVE-2016-3074

[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

9525 - Cisco IOS Virtual LAN 802.1q Frame Injection Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Medium

CVE: CVE-1999-1129

Update Details

Recommendation is updated

9534 - Cisco IOS Large TCP Scan Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Medium

CVE: CVE-2002-2052

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

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

16876 - BlackBerry Link OpenSSL Multiple Vulnerabilities

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

Risk Level: Medium

CVE: CVE-2010-5298, CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470

[Update Details](#)

Recommendation is updated Documentation is updated

16877 - BlackBerry Link OpenSSL Multiple Vulnerabilities

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2010-5298, CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470

[Update Details](#)

Recommendation is updated Documentation 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

17844 - (MS15-015) Vulnerability in Microsoft Windows Could Allow Elevation of Privilege (3031432)

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

Risk Level: Medium

CVE: CVE-2015-0062

Update Details

Recommendation is updated

17847 - (MS15-016) Vulnerability in Microsoft Graphics Component Could Allow Information (3029944)

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

Risk Level: Medium

CVE: CVE-2015-0061

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

19959 - (VMSA-2016-0004) VMware vRealize Automation Session Content Spoofing Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-2076

Update Details

Risk is updated

19960 - (VMSA-2016-0004) VMware vCenter Server Session Content Spoofing Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2016-2076

Update Details

Risk is updated

19961 - (VMSA-2016-0004) VMware vCenter Server Session Content Spoofing Vulnerability

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

Risk Level: Medium

CVE: CVE-2016-2076

Update Details

Risk 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

8317 - Cisco TFTP Server Denial of Service Vulnerability

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

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

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

8666 - Cisco IOS HTTP Server Cross Site Scripting Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Medium

CVE: CVE-2009-0470

[Update Details](#)

Recommendation is updated Documentation is updated

8671 - Cisco IOS HTTP Server Cross Site Request Forgery Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Medium

CVE: CVE-2009-0471

[Update Details](#)

Recommendation is updated Documentation 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

9561 - Cisco IOS Regular Expression Engine Denial Of Service Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Medium

CVE: CVE-2007-4430

[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

9911 - Cisco IOS TACACS+ Body Length Buffer Overflow Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Medium

CVE: CVE-2000-0486

[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

11240 - (MS11-009) Microsoft Scripting Engines Information Disclosure (2475792)

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

Risk Level: Medium

CVE: CVE-2011-0031

Update Details

Recommendation is updated

11255 - (MS11-009) Vulnerability In JScript And VBScript Scripting Engines Could Allow Information Disclosure (2475792)

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

Risk Level: Medium

CVE: CVE-2011-0031

Update Details

Recommendation is updated

11722 - Citrix MetaFrame Client Specified Published Applications Enumeration Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Miscellaneous

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

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

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

12669 - Carel Industries PlantVisor Enhanced Directory Traversal Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> SCADA
Risk Level: Medium
CVE: CVE-2011-3487

[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

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

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.aspx 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

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

14971 - Cisco Linksys EA2700 Multiple Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

15134 - D-Link DIR-635 "data" Cross-Site Scripting and Cross-Site Request Forgery Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Wireless

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[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

15619 - Cisco Prime Network Control System (NCS) Health Monitor Login Page Cross-Site Scripting Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-2012-5990

[Update Details](#)

Recommendation is updated

15704 - (MS13-085) Microsoft Excel Memory Corruption Remote Code Execution II (2885080)

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

Risk Level: Medium

CVE: CVE-2013-3890

[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

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

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

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

15962 - Cisco Adaptive Security Appliance Software Phone Proxy Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-6682

[Update Details](#)

Recommendation is updated

15963 - Cisco Adaptive Security Appliance Software Auto-Update Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2013-5568

[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

16025 - (MS13-104) Vulnerability in Microsoft Office Could Allow Information Disclosure (2909976)

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

Risk Level: Medium

CVE: CVE-2013-5054

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

16038 - (MS13-104) Microsoft Office Token Hijacking Information Disclosure (2909976)

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

Risk Level: Medium
CVE: CVE-2013-5054

[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

16270 - Cisco NX-OS Software Label Distribution Protocol Message Denial of Service

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous
Risk Level: Medium
CVE: CVE-2014-0677

[Update Details](#)

Recommendation is updated

16271 - Cisco NX-OS Software TACACS+ Command Authorization Local Security Bypass

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-0676

[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

16386 - Cisco Adaptive Security Appliance Phone Proxy sec_db Race Condition Security Bypass

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-0739

[Update Details](#)

Recommendation is updated

16457 - Cisco Adaptive Security Appliance WebVPN Login Page Cross-Site Scripting

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2014-2120

[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

16603 - (MS14-023) Microsoft Office Chinese Grammar Checking Remote Code Execution (2961037)

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

Risk Level: Medium

CVE: CVE-2014-1756

[Update Details](#)

Recommendation is updated

16605 - (MS14-023) Microsoft Office Token Reuse Remote Code Execution (2961037)

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

Risk Level: Medium

CVE: CVE-2014-1808

[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

16933 - DotNetNuke Multiple Modules Arbitrary File Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Web Server

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

17039 - BlackBerry OS OpenSSL Multiple Vulnerabilities

Category: Wireless Assessment -> NonIntrusive -> Blackberry

Risk Level: Medium

CVE: CVE-2010-5298, CVE-2014-0195, CVE-2014-0198, CVE-2014-0221, CVE-2014-0224, CVE-2014-3470

[Update Details](#)

Recommendation is updated Documentation 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

17415 - FESTO Robotino View Unspecified Defect Remote Denial of Service

Category: Windows Host Assessment -> SCADA

(CATEGORY REQUIRES CREDENTIALS)

Risk Level: Medium

CVE: CVE-MAP-NOMATCH

[Update Details](#)

Recommendation is updated

17481 - (MS14-085) Vulnerability in Microsoft Graphics Component Could Allow Information (3013126)

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

Risk Level: Medium

CVE: CVE-2014-6355

[Update Details](#)

Recommendation is updated

17492 - (MS14-085) Microsoft Graphics ASLR Bypass Information Disclosure (3013126)

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

Risk Level: Medium

CVE: CVE-2014-6355

[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

17842 - (MS15-015) Microsoft Windows Create Process Privilege Escalation (3031432)

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

Risk Level: Medium

CVE: CVE-2015-0062

Update Details

Recommendation is updated

17845 - (MS15-016) Microsoft Windows TIFF Processing Information Disclosure (3029944)

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

Risk Level: Medium

CVE: CVE-2015-0061

Update Details

Recommendation is updated

17981 - (MS15-024) Vulnerability in PNG Processing Could Allow Information Disclosure (3035132)

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

Risk Level: Medium

CVE: CVE-2015-0080

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

18003 - (MS15-024) Microsoft Windows PNG Malformed Parsing Information Disclosure (3035132)

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

Risk Level: Medium

CVE: CVE-2015-0080

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

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

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

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

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

19318 - (VMSA-2015-0008) VMware Horizon View Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2015-3269, CVE-2015-5255

Update Details

CVE is updated

19323 - (VMSA-2015-0008) VMware vCenter Server Information Disclosure Vulnerability

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

Risk Level: Medium

CVE: CVE-2015-3269, CVE-2015-5255

Update Details

CVE is updated

19324 - (VMSA-2015-0008) VMware vCenter Server Information Disclosure Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium

CVE: CVE-2015-3269, CVE-2015-5255

Update Details

CVE 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

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

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

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

130472 - Debian Linux 7.0 DSA-3553-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2015-8852

[Update Details](#)

Risk is updated

144522 - SuSE Linux 13.2 openSUSE-SU-2016:1007-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3190

[Update Details](#)

Risk is updated

144543 - SuSE SLES 12, 12 SP1, SLED 12, 12 SP1 SUSE-SU-2016:1100-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-3190

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

12473 - (MS11-069) Microsoft .NET Framework Socket Restriction Bypass Could Allow Information Disclosure (2567951)

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

Risk Level: Medium

CVE: CVE-2011-1978

Update Details

Recommendation is updated

12476 - (MS11-069) Vulnerability in .NET Framework Could Allow Information Disclosure (2567951)

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

Risk Level: Medium

CVE: CVE-2011-1978

Update Details

Recommendation is updated

16384 - Cisco Adaptive Security Appliance Phone Proxy CTL Security Bypass Vulnerability

Category: SSH Module -> NonIntrusive -> SSH Miscellaneous

Risk Level: Medium
CVE: CVE-2014-0738

[Update Details](#)

Recommendation is updated

16999 - (MS14-045) Microsoft Windows Kernel Pool Allocation Information Disclosure (2984615)

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

Risk Level: Medium
CVE: CVE-2014-4064

[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

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

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

18308 - (MS15-053) Vulnerabilities in JScript and VBScript Scripting Engines Could Allow Security (3057263)

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

Risk Level: Medium

CVE: CVE-2015-1684, CVE-2015-1686

[Update Details](#)

Recommendation is updated

18309 - (MS15-053) Microsoft VBScript Scripting Engine ASLR I Security Bypass (3057263)

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

Risk Level: Medium

CVE: CVE-2015-1684

[Update Details](#)

Recommendation is updated

18310 - (MS15-053) Microsoft VBScript Scripting Engine ASLR II Security Bypass (3057263)

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

Risk Level: Medium

CVE: CVE-2015-1686

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

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

19070 - (MS15-108) Microsoft VBScript and JScript ASLR Security Bypass (3089659)

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

Risk Level: Medium
CVE: CVE-2015-6052

[Update Details](#)

Recommendation is updated

19071 - (MS15-108) Microsoft VBScript and JScript Information Disclosure (3089659)

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

Risk Level: Medium
CVE: CVE-2015-6059

[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

19351 - (MS15-134) Microsoft Windows Media Center Information Disclosure (3108669)

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

Risk Level: Medium
CVE: CVE-2015-6127

[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

88773 - Slackware Linux 14.0, 14.1 SSA:2016-121-01 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2167, CVE-2016-2168

[Update Details](#)

Risk is updated

130483 - Debian Linux 8.0 DSA-3561-1 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2167, CVE-2016-2168

[Update Details](#)

Risk is updated

181938 - FreeBSD subversion Multiple Vulnerabilities (c8174b63-0d3a-11e6-b06e-d43d7eed0ce2)

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

Risk Level: Medium

CVE: CVE-2016-2167, CVE-2016-2168

[Update Details](#)

Risk is updated

190359 - Fedora Linux 23 FEDORA-2016-1642a20327 Update Is Not Installed

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

Risk Level: Medium

CVE: CVE-2016-2550

Update Details

Risk is updated

9583 - Cisco IOS Online Help Information Disclosure Vulnerability

Category: General Vulnerability Assessment -> NonIntrusive -> Network

Risk Level: Low

CVE: CVE-2000-0345

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

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

144541 - SuSE Linux 13.2 openSUSE-SU-2016:1101-1 Update Is Not Installed

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

Risk Level: Low

CVE: CVE-2014-9770, CVE-2015-8842

Update Details

Risk 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

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.

MCAFFEE 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