Monthly Security Bulletin and Security Advisory Briefing| November 2013

Teresa Ghiorzoe
Security Program Manager- GBS LATAM

Alejandro Leal Rodriguez
Technical Support Lead - LATAM

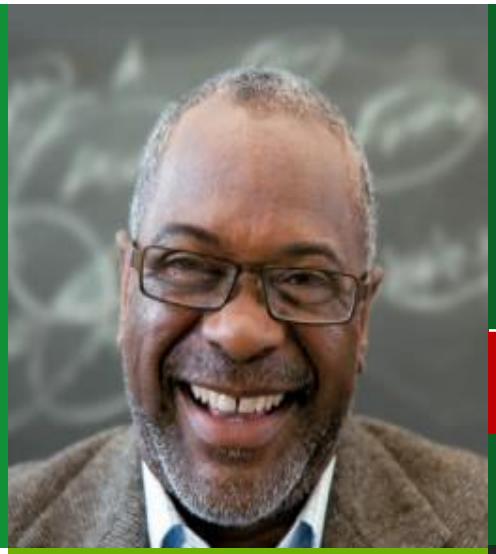
Blog de Seguridad: :
http://blogs.technet.com/b/seguridad/

Twitter: LATAMSRC
Email: LATAMSRC@Microsoft.com

CSS Security Worldwide Programs

Microsoft

November 2013 Agenda



New Security Bulletins

8

Critical	Important
3	5

3 New Security Advisories

2 Rereleased Security Advisories

Other Security Resources

- ✓ Detection and Deployment Table
- ✓ Product Support Lifecycle Information
- ✓ Post Release Issue Tracking, Escalations, and Contacts
- ✓ Slide Decks and the Public Webcast

CSS Security Worldwide Programs

Microsoft

November 2013 Security Bulletins

Bulletin	Impact	Component	Severity	Priority	Exploit Index	Public
MS13-088	Remote Code Execution	Internet Explorer	Critical	1	1	No
MS13-089	Remote Code Execution	GDI	Critical	1	1	No
MS13-090	Remote Code Execution	Kill Bits	Critical	1	1	No
MS13-091	Remote Code Execution	Office	Important	2	1	No
MS13-092	Elevation of Privilege	Hyper-V	Important	2	1	No
MS13-093	Information Disclosure	AFD	Important	2	3	No
MS13-094	Information Disclosure	Outlook	Important	3	3	Yes
MS13-095	Denial of Service	XML	Important	3	3	No

Exploitability Index: 1 - Exploit code likely | 2 - Exploit code difficult | 3 - Exploit code unlikely | NA - Not Affected | * - Not Rated

CSS Security Worldwide Programs

Microsoft

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

Affected Software

- Internet Explorer 6 on Windows XP and Windows Server 2003.
- Internet Explorer 7 on Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.
- Internet Explorer 8 on Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.
- Internet Explorer 9 on Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.
- Internet Explorer 10 on Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, and Windows RT.
- Internet Explorer 11 on Windows 8.1, Windows Server 2012 R2, and Windows RT 8.1.

Note: Internet Explorer 11 Preview for Windows 8.1 Preview and Windows RT 8.1 Preview are both affected by this bulletin. The updates are available on Windows Update.

Severity | Critical

Deployment Priority	Update Replacement	More Information and / or Known Issues
1	MS13-080	None

Restart Requirement

✓ A restart is required

Uninstall Support

✓ Use Add or Remove Programs in Control Panel

Detection and Deployment

WU	MU	MBSA	WSUS	ITMU	SCCM
Yes	Yes	Yes [1] [2]	Yes [2]	Yes [2]	Yes [2]

1. The Microsoft Baseline Security Analyzer (MBSA) 2.3 for Windows 8 or Windows Server 2012 is available as a beta this month.
2. Windows RT devices can only be serviced with Windows and Microsoft Update and the Microsoft Store.

CSS Security Worldwide Programs

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

Vulnerability Details

- One information disclosure vulnerability exists in the way that Internet Explorer handles specially crafted web content when generating print previews.
- One information disclosure vulnerability exists in the way that Internet Explorer processes CSS special characters.
- Eight remote code execution vulnerabilities exist when Internet Explorer improperly accesses an object in memory. These vulnerabilities could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-3908	Important	Information Disclosure	NA	3	NA	No	No	None
CVE-2013-3909	Important	Information Disclosure	NA	3	NA	No	No	None
CVE-2013-3871,3910,3911	Critical	Remote Code Execution	NA	1	NA	No	No	None
CVE-2013-3912,3914,3915,3916	Critical	Remote Code Execution	1	1	NA	No	No	None
CVE-2013-3917	Critical	Remote Code Execution	1	2	NA	No	No	None

Exploitability Index: 1 - Exploit code likely | 2 - Exploit code difficult | 3 - Exploit code unlikely | NA - Not Affected | * - Not Rated
DoS Rating: T = Temporary (DoS ends when an attack ceases) | P = Permanent (Administrative action required to recover)

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

Vulnerability Details (cont'd)

Attack Vectors

All

- Attacker hosts a malicious website utilizing the vulnerability, then convinces users to visit the site.
- Attacker takes advantage of compromised websites and/or sites hosting ads from other providers.

CVE-2013-3908

- An attacker could use active scripting to initiate the print preview of a specially crafted webpage

Mitigations

All

Users would have to be persuaded to visit a malicious website.

All except CVE-2013-3908 and CVE-2013-3909

- Exploitation only gains the same user rights as the logged-on account.
- By default, all Microsoft email clients open HTML email messages in the Restricted Sites zone.
- By default, IE runs in a restricted mode for all Windows Servers.

Workarounds

CVE-2013-3908:

- Do not use the Print Preview feature in Internet Explorer .

All except CVE-2013-3909:

- Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones.
- Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone.

CVE-2013-3909:

- Microsoft has not identified any workarounds for this vulnerability.

Microsoft

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

Affected Software

All editions of:

- ✓ Windows XP
- ✓ Windows Server 2003
- ✓ Windows Vista
- ✓ Windows Server 2008
- ✓ Windows 7
- ✓ Windows Server 2008 R2
- ✓ Windows 8
- ✓ Windows 8.1
- ✓ Windows Server 2012
- ✓ Windows 2012 R2
- ✓ Windows RT
- ✓ Windows RT 8.1

Severity | Critical

Deployment Priority	Update Replacement	More Information and / or Known Issues
1	MS08-071	No

Restart Requirement

- ✓ A restart is required

Uninstall Support

- ✓ Use Add or Remove Programs in Control Panel

Detection and Deployment

WU	MU	MBSA	WSUS	ITMU	SCCM
Yes	Yes	Yes [1] [2]	Yes [2]	Yes [2]	Yes [2]

http://blogs.technet.com/b/msrc/archive/2013/11/07/clarification-on-security-advisory-2896666-and-the-ans-for-the-november-2013-security-bulletin-release.aspx

1. The Microsoft Baseline Security Analyzer v2.3 is in beta and now supports Windows 8 or Windows Server 2012
2. Windows RT devices can only be serviced with Windows and Microsoft Update and the Microsoft store

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

Vulnerability Details

A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) processes specially crafted image files.

The vulnerability is caused by a memory corruption when the Windows Graphics Device Interface improperly processes a specially crafted image contained in a Windows Write (.wri) file.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-3091	Critical	Remote Code Execution	1	1	NA	No	No	None

Attack Vectors

- ✓ Attacker hosts a malicious website that contains specially crafted Windows Write file, then convinces users to visit the site
- ✓ Attacker takes advantage of compromised websites and/or sites hosting ads from other providers

Mitigations

- ✓ The vulnerability cannot be exploited automatically through email.
- ✓ Users would have to be persuaded to visit a malicious website.
- ✓ Exploitation only gains the same user rights as the logged-on account

Workarounds

- ✓ Disable the Word 6 converter by restricting access to mswrd8.wpc.
- ✓ Do not open Microsoft Write (.wri) documents that you receive from untrusted sources or that you receive unexpectedly from trusted sources.

Exploitability Index: 1 - Exploit code likely | 2 - Exploit code difficult | 3 - Exploit code unlikely | NA - Not Affected | * - Not Rated
DoS Rating: T = Temporary (DoS ends when an attack ceases) | P = Permanent (Administrative action required to recover)

Microsoft

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

Affected Software

- ✓ Windows XP
- ✓ Windows Server 2003
- ✓ Windows Vista
- ✓ Windows Server 2008
- ✓ Windows 7
- ✓ Windows Server 2008 R2
- ✓ Windows 8
- ✓ Windows 8.1
- ✓ Windows Server 2012
- ✓ Windows Server 2012 R2
- ✓ Windows RT
- ✓ Windows RT 8.1

Severity | Critical

Deployment Priority	Update Replacement	More Information and / or Known Issues
1	MS11-090	None

Restart Requirement

- ✓ A restart may be required

Uninstall Support

- ✓ Use Add or Remove Programs in Control Panel

Detection and Deployment

WU	MU	MBSA	WSUS	ITMU	SCCM
Yes	Yes	Yes [1] [2]	Yes [2]	Yes [2]	Yes [2]

http://blogs.technet.com/b/msrc/archive/2013/11/11/activex-control-issue-being-addressed-in-update-tuesday.aspx

1. The Microsoft Baseline Security Analyzer v2.3 is in beta and now supports Windows 8 or Windows Server 2012
2. Windows RT devices can only be serviced with Windows and Microsoft Update and the App Store.

CSS Security Worldwide Programs

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

Vulnerability Details

- A remote code execution vulnerability exists in the InformationCardSigninHelper Class ActiveX control, icardie.dll. An attacker could exploit the vulnerability by constructing a specially crafted webpage. When a user views the webpage, the vulnerability could allow remote code execution.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-3918	Critical	Remote Code Execution	1	1	NA	NA	Yes- Limited	None

Attack Vectors

- A specially crafted website.

Mitigations

- Users would have to be persuaded to visit a malicious website.
- By default, all Microsoft email clients open HTML email messages in the Restricted Sites zone.
- Exploitation only gains the same user rights as the logged-on account.
- By default, Internet Explorer on Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 runs in a restricted mode.

Workarounds

- Prevent COM objects from running in Internet Explorer.

Exploitability Index: 1 - Exploit code likely | 2 - Exploit code difficult | 3 - Exploit code unlikely | NA - Not Affected | * - Not Rated
DoS Rating: T = Temporary (DoS ends when an attack ceases) | P = Permanent (Administrative action required to recover)

Microsoft

MS13-091 Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2885093)

Affected Software

- Office 2003
- Office 2007
- Office 2010
- Office 2013
- Office 2013 RT

Severity | Important

Deployment Priority	Update Replacement	More Information and / or Known Issues
2	MS09-073	None

Restart Requirement

✓ A restart may be required

Uninstall Support

✓ Use Add or Remove Programs in Control Panel

Detection and Deployment

WU	MU	MBSA	WSUS	ITMU	SCCM
No	Yes	Yes	Yes	Yes	Yes

Note: Windows RT devices can only be serviced with Windows and Microsoft Update and the Microsoft store

CSS Security Worldwide Programs

MS13-091 Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2885093)

Vulnerability Details

- A remote code execution vulnerability exists in the way that affected Microsoft Office software parses specially crafted WPD files. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-0082	Important	Remote Code Execution	NA	3	NA	No	No	None
CVE-2013-1324	Important	Remote Code Execution	1	1	NA	No	No	None
CVE-2013-1325	Important	Remote Code Execution	NA	1	NA	No	No	None

Attack Vectors

- A specially crafted Office file
- ✓ Common delivery mechanisms: a maliciously crafted webpage, an email attachment, an instant message, a peer-to-peer file share, a network share, and/or a USB thumb drive.

Mitigations

- The vulnerability cannot be exploited automatically through email because a user must open an attachment that is sent in an email message.
- Users would have to be persuaded to visit a malicious website.
- Exploitation only gains the same user rights as the logged-on account

Workarounds

- Restrict access to the affected WordPerfect file converter (wpft632.cnv)
- Do not open Office files that you receive from untrusted sources or that you receive unexpectedly from trusted sources.

Exploitability Index: 1 - Exploit code likely | 2 - Exploit code difficult | 3 - Exploit code unlikely | NA - Not Affected | * - Not Rated
DoS Rating: T = Temporary (DoS ends when an attack ceases) | P = Permanent (Administrative action required to recover)

Microsoft

MS13-092 Vulnerability in Hyper-V Could Allow Elevation of Privilege (2893986)

Affected Software

- Windows 8 x64
- Windows Server 2012

Severity | Important

Deployment Priority	Update Replacement	More Information and / or Known Issues
2	None	None

Restart Requirement

✓ A restart is required

Uninstall Support

✓ Use Add or Remove Programs in Control Panel

Detection and Deployment

WU	MU	MBSA	WSUS	ITMU	SCCM
Yes	Yes	Yes	Yes	Yes	Yes

The Microsoft Baseline Security Analyzer v2.3 is in beta and now supports Windows 8 or Windows Server 2012

CSS Security Worldwide Programs

Microsoft

MS13-092 Vulnerability in Hyper-V Could Allow Elevation of Privilege (2893986)

Vulnerability Details

- An elevation of privilege vulnerability exists in Hyper-V on Windows 8 and Windows Server 2012. An attacker who successfully exploited this vulnerability could execute arbitrary code as System in another virtual machine (VM) on the shared Hyper-V host. An attacker would not be able to execute code on the Hyper-V host, only on guest VMs on the same host. The vulnerability could also allow denial of service in Hyper-V on the same platforms, allowing an attacker to cause the Hyper-V host to stop responding or restart.
- The vulnerability is caused when the value of a data structure is not properly verified, allowing a memory address with an invalid address to be used.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-3898	Important	Elevation of Privilege	NA	1	P	No	No	None

Attack Vectors

- A specially crafted function parameter passed from VM to hypervisor.

Mitigations

- Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

- Microsoft has not identified any workarounds for this vulnerability.

Exploitability Index: 1 - Exploit code likely | 2 - Exploit code difficult | 3 - Exploit code unlikely | NA - Not Affected | * - Not Rated
DoS Rating: T = Temporary (DoS ends when an attack ceases) | P = Permanent (Administrative action required to recover)

Microsoft

MS13-093 Vulnerability in Windows Ancillary Function Driver Could Allow Information Disclosure (2875783)

Affected Software

- Windows XP x64 SP2
- Windows Server 2003
  - → x64 SP2
  - → Itanium SP2
- Windows Vista x64 SP2
- Windows Server 2008
  - → x64 SP2
  - → Itanium SP2
- Windows 7 x64 SP1
- Windows Server 2008 R2
  - → x64 SP1
  - → Itanium SP1
- Windows 8 x64
- Windows Server 2012

Severity | Important

Deployment Priority	Update Replacement	More Information and / or Known Issues
2	MS12-009	None

Restart Requirement

✓ A restart is required

Uninstall Support

✓ Use Add or Remove Programs in Control Panel

Detection and Deployment

WU	MU	MBSA	WSUS	ITMU	SCCM
Yes	Yes	Yes [1]	Yes [1]	Yes [1]	Yes [1]

The Microsoft Baseline Security Analyzer v2.3 is in beta and now supports Windows 8 or Windows Server 2012

CSS Security Worldwide Programs

Microsoft

MS13-093 Vulnerability in Windows Ancillary Function Driver Could Allow Information Disclosure (2875783)

Vulnerability Details

An information disclosure vulnerability exists when the Windows kernel-mode driver improperly handles copying data between kernel and user memory.

The update addresses the vulnerability by correcting how Windows copies data from kernel memory to user memory.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-3887	Important	Information Disclosure	NA	3	3NA	No	No	None

Attack Vectors

- Attacker logs on locally and runs a specially crafted application to get information from a higher privileged account.

Mitigations

- An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability.

Workarounds

- Don't open executables from untrusted sources.

Exploitability Index: 1 - Exploit code likely | 2 - Exploit code difficult | 3 - Exploit code unlikely | NA - Not Affected | * - Not Rated
DoS Rating: T = Temporary (DoS ends when an attack ceases) | P = Permanent (Administrative action required to recover)

Microsoft

MS13-094 Vulnerability in Microsoft Outlook Could Allow Information Disclosure (2894514)

Affected Software

- ✓ Microsoft Office 2007 SP3
- ✓ Microsoft Office 2010 SP1 and SP2
- ✓ Microsoft Outlook 2013
- ✓ Microsoft Outlook 2013 RT

Severity | Important

Deployment Priority	Update Replacement	More Information and / or Known Issues
3	MS13-068	Yes

Restart Requirement

- ✓ A restart may be required

Uninstall Support

- ✓ Use Add or Remove Programs in Control Panel

Detection and Deployment

WU	MU	MBSA	WSUS	ITMU	SCCM
No	Yes	Yes	Yes	Yes	Yes

Windows RT devices can only be serviced with Windows and Microsoft Update and the Microsoft store

CSS Security Worldwide Programs

MS13-094 Vulnerability in Microsoft Outlook Could Allow Information Disclosure (2894514)

Vulnerability Details:

An information disclosure vulnerability when Microsoft Outlook does not properly handle the expansion of S/MIME certificate metadata. An attacker who successfully exploited this vulnerability could ascertain system information, such as the IP address and open TCP ports, from the target system and other systems that share the network with the target system.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-3905	Important	Information Disclosure	3	3	NA	Yes	No	None

Attack Vectors

- A specially crafted S/MIME certificate sent in an email message.

Mitigations

- Microsoft has not identified any mitigating factors for this vulnerability.

Workarounds

- Disable the Reading Pane in Outlook.

Exploitability Index: 1 - Exploit code likely | 2 - Exploit code difficult | 3 - Exploit code unlikely | NA - Not Affected | * - Not Rated
DoS Rating: T = Temporary (DoS ends when an attack ceases) | P = Permanent (Administrative action required to recover)

Microsoft

MS13-095 Vulnerability in Digital Signatures Could Allow Denial of Service (2868626)

Affected Software:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2
- Windows RT
- Windows RT 8.1

Severity | Important

Deployment Priority	Update Replacement	More Information and / or Known Issues
3	2661254	None

Restart Requirement

✓ This update requires a restart

Uninstall Support

✓ Use Add or Remove Programs in Control Panel

Detection and Deployment

WU	MU	MBSA	WSUS	ITMU	SCCM
Yes	Yes	Yes [1 | 2]	Yes [2]	Yes [2]	Yes [2]

1. The Microsoft Baseline Security Analyzer v2.3 is in beta and now supports Windows 8 or Windows Server 2012.
2. Windows RT devices can only be serviced with Windows and Microsoft Update and the Windows App Store.

CSS Security Worldwide Programs

MS13-095 Vulnerability in Digital Signatures Could Allow Denial of Service (2868626)

Vulnerability Details:

- A denial of service vulnerability exists in implementations of X.509 certificate parsing that could cause the service to stop responding. The vulnerability is caused when the X.509 certificate validation operation fails to handle a specially crafted X.509 certificate.
- An attacker who successfully exploited this vulnerability could cause the web service performing certificate validation to become non-responsive.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-3869	Important	Denial of Service	3	3	T	No	No	None

Attack Vectors

- A specially crafted X.509 certificate sent to a web service.

Mitigations

- Microsoft has not identified any mitigations for this vulnerability.

Workarounds

- Microsoft has not identified any workarounds for this vulnerability.

Exploitability Index: 1 - Exploit code likely | 2 - Exploit code difficult | 3 - Exploit code unlikely | NA - Not Affected | * - Not Rated
DoS Rating: T = Temporary (DoS ends when an attack ceases) | P = Permanent (Administrative action required to recover)

New Security Advisories

Security Advisory (2862152)

Vulnerability in Direct Access Could Allow Security Feature Bypass

- ✓ Microsoft is announcing the availability of an update for supported editions of Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows RT, Windows 8, Windows 8.1, Windows Server 2012 and Windows Server 2012 R2 to address a vulnerability in how Direct Access authenticates Direct Access server connections to Direct Access clients.
- ✓ An attacker who successfully exploited the vulnerability could use a specially crafted Direct Access server to pose as a legitimate Direct Access Server in order to establish connections with legitimate Direct Access clients.

Security Advisory (2868725)

Update for Disabling RC4

Microsoft is announcing the availability of an update that restricts the use of certificates with MD5 hashes.

- ✓ Microsoft is announcing the availability of an update for supported editions of Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, and Windows RT. The update supports the removal of RC4 as an available cipher on affected systems through registry settings. It allows developers to remove RC4 in individual applications through the use of the SCH_USE_STRONG_CRYPTO flag in the SCHANNEL_CRED structure. These options are not enabled by default.
- ✓ Use of RC4 encryption in TLS and SSL could allow an attacker to perform man-in-the-middle attacks and recover plaintext from encrypted sessions.

Rereleased Security Advisories

Security Advisory (2755801) Update for Vulnerabilities in Adobe Flash Player in Internet Explorer

- ✓ On November 12, 2013, Microsoft released an update (2898108) for Internet Explorer on all supported editions of Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows RT, and Windows RT 8.1. The update addresses the vulnerabilities described in Adobe Security bulletin APSB13-26 For more information about this update, including download links, see Microsoft Knowledge Base Article 2898108.

Security Advisory (2854544)

Updates to Improve Cryptography and Digital Certificate Handling in Windows

- ✓ Microsoft released an update (2868725) for all supported editions of Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, and Windows RT to address known weaknesses in RC4. The update is offered via automatic updating and through the Microsoft Update service for all affected software. The update is also available on the Download Center as well as the Microsoft Update Catalog for all affected software except Windows RT.
- ✓ Microsoft announced a policy change to the Microsoft Root Certificate Program for the deprecation of the SHA-1 hashing algorithm in X.509 digital certificates. The new policy will no longer allow root certificate authorities to issue X.509 certificates using the SHA-1 hashing algorithm for the purposes of SSL and code signing after January 1, 2016. Microsoft recommends that customers replace their SHA-1 certificates with SHA-2 certificates at the earliest opportunity. For more information, see Microsoft Security Advisory 2880823.

Microsoft

High impact non-security releases

Internet Explorer 11 on Windows 7

- Internet Explorer 11 FAQ
  http://technet.microsoft.com/library/dn268945.aspx
- Internet Explorer 11 Blocker Toolkit
  http://go.microsoft.com/fwlink/?LinkId=328195

Microsoft

Microsoft Support Lifecycle

Lifecycle Changes

The following product families and service pack levels are scheduled to have their support lifecycle expire on November 12, 2013

Product Family

- Forefront Threat Management Gateway, Medium Business Edition (mainstream support ends)

Will expire January 14, 2014:

- Live Communications Server 2003

Remember that support for the entire Windows XP product family will expire on 4/8/2014

✓ http://support.microsoft.com/lifecycle

CSS Security Worldwide Programs

Microsoft

November 2013 Security Bulletins

Bulletin	Description	Severity	Priority
MS13-088	Cumulative Security for Internet Explorer (2888505)	Critical	1
MS13-089	Vulnerability in Windows Graphics Device Interface Could Allow Remote Code Execution	Critical	1
MS13-090	Cumulative Security Update of ActiveX Kill Bits	Critical	1
MS13-091	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution	Important	2
MS13-092	Vulnerability in Hyper-V Could Allow Elevation of Privilege	Important	2
MS13-093	Vulnerability in Windows Ancillary Function Driver Could Allow Information Disclosure	Important	2
MS13-094	Vulnerability in Microsoft Outlook Could Allow Information Disclosure	Important	3
MS13-095	Vulnerability in XML Digital Signatures Could Allow Denial of Service	Important	3

Appendix

CSS Security Worldwide Programs

Malicious Software Removal Tool (MSRT) Updates

MSRT Changes

New malware families added to the November 2013 MSRT

Win32/Deminnix

- A family of trojans that perform bitcoin mining on an affected system and may modify the users browser settings.

Win32/Napolar

- A family of trojans that performs file download, ddos attack, network traffic monitoring for FTP/POP3/Web credentials, also deploys user-mode rootkit for hiding its presence.

Additional Tools

Microsoft Safety Scanner

- Same basic engine as the MSRT, but with a full set of A/V signatures

Windows Defender Offline

- An offline bootable A/V tool with a full set of signatures
- Designed to remove rootkits and other advanced malware that can't always be detected by antimalware programs
- Requires you to download an ISO file and burn a CD, DVD, or USB flash drive

Microsoft

November 2013 Manageability Tools Reference

Bulletin	Windows Update	Microsoft Update	MBSA	WSUS	SMS ITMU	SCCM
MS13-088	Yes	Yes	Yes [1]	Yes [1]	Yes [1]	Yes [1]
MS13-089	Yes	Yes	Yes [1]	Yes [1]	Yes [1]	Yes [1]
MS13-090	Yes	Yes	Yes [1]	Yes [1]	Yes [1]	Yes [1]
MS13-091	No [2]	Yes	Yes [2]	Yes [2]	Yes [2]	Yes [2]
MS13-092	Yes	Yes	Yes	Yes	Yes	Yes
MS13-093	Yes	Yes	Yes	Yes	Yes	Yes
MS13-094	No [2]	Yes	Yes [2]	Yes [2]	Yes [2]	Yes [2]
MS13-095	Yes	Yes	Yes [1]	Yes [1]	Yes [1]	Yes [1]

Note: The Microsoft Baseline Security Analyzer v2.3 is in beta to support Windows 8 or Windows Server 2012

1. Windows RT devices can only be serviced with Windows and Microsoft Update and the Microsoft Store
2. Microsoft Office 2013 RT is available through Windows Update.

November 2013 Non-Security Content

Description	Classification	Deployment
System Update Readiness Tool for Windows 7 (KB947821) [November 2013]	Critical Updates	Site, AU, SUS, Catalog
Update for Windows 8 (KB2883201)	Critical Updates	Site, AU, SUS, Catalog
Update for Windows 8.1 (KB2904594) Internal SH	Critical Updates	Site, AU
Update for Windows RT 8.1 (KB2905029)	Critical Updates	Site, AU
Update for Root Certificates for Windows 7 [November 2013] (KB931125)	Updates	SUS, Catalog
Update for Windows 7 (KB2515325)	Updates	Site, SUS, Catalog
Update for Windows 7 (KB2647753)	Updates	Site, SUS, Catalog
Update for Windows 7 (KB2830477)	Updates	Site, SUS, Catalog
Update for Windows 7 (KB2893519)	Updates	Site, SUS, Catalog
Update for Windows 8 (KB2882780)	Updates	Site, SUS, Catalog
Update for Windows 8 (KB2889784)	Updates	Site, SUS, Catalog
Update for Windows 8.1 (KB2890140)	Updates	Site, SUS, Catalog
Update for Windows Home Server 2011 (KB2885314)	Updates	Site
Update for Windows Small Business Server 2011 Essentials (KB2885313)	Updates	Site
Update for Windows Storage Server 2008 R2 Essentials (KB2885315)	Updates	Site, SUS
Update Rollup 4 for Windows Small Business Server 2011 Standard (KB2885319)	Update Rollups	Site, AU, SUS, Catalog

November 2013 Non-Security Content (cont'd)

Description	Classification	Deployment
Update for Microsoft Lync 2013 (KB2817678) 32-Bit Edition	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft Lync 2013 (KB2825630) 32-Bit Edition	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft Office 2010 (KB2589352) 32-Bit Edition	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft Office 2010 (KB2597087) 32-Bit Edition	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft Office 2013 (KB2827239) 32-Bit Edition	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft Office 2013 (KB2837643) 32-Bit Edition	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft Office 2013 (KB2837649) 32-Bit Edition	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft Office Outlook 2007 Junk Email Filter (KB2825642)	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft OneNote 2013 (KB2837642) 32-Bit Edition	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft SharePoint Enterprise Server 2013 (KB2726989)	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft SharePoint Enterprise Server 2013 (KB2737991)	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft SharePoint Enterprise Server 2013 (KB2837628)	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft SharePoint Enterprise Server 2013 (KB2837657)	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft SkyDrive Pro (KB2837652) 32-Bit Edition	Critical Updates	Site, AU, SUS, Catalog
Update for Microsoft Word 2013 (KB2837630) 32-Bit Edition	Critical Updates	Site, AU, SUS, Catalog
Update for Outlook 2003 Junk E-mail Filter (KB2849999)	Critical Updates	Site, AU, SUS, Catalog
Definition Update for Microsoft Office 2010 (KB982726) 32-Bit Edition	Definition Updates	Site, AU, SUS, Catalog
Definition Update for Microsoft Office 2013 (KB2760587) 32-Bit Edition	Definition Updates	Site, AU, SUS, Catalog

November 2013 Non-Security Content

Description	Classification	Deployment
Update for Lync 2010 X64 (KB2884632)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup for Lync Server 2010 (KB2889610)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup for Lync Server 2010 Conferencing Server (KB2889609)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup for Lync Server 2010 Core Components (KB2884613)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup for Lync Server 2010 Web Components Server (KB2884619)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup for Lync Server 2013 (KB2881684)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup for Lync Server 2013 Call Park Service (KB2881703)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup for Lync Server 2013 Conferencing Announcement Service (KB2881701)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup for Lync Server 2013 Conferencing Attendant (KB2881700)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup for Lync Server 2013 Core Components (KB2881682)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup for Lync Server 2013 Core Management Server (KB2883679)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup for Lync Server 2013 Mediation Server (KB2881699)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup for Lync Server 2013 Unified Communications Managed API 4.0 Core Runtime x64 (KB2881685)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup for Lync Server 2013 Web Components Server (KB2881688)	Update Rollups	Site, AU, SUS, Catalog
Update Rollup 15 for Microsoft Dynamics CRM 2011 for Outlook (KB2843571)	Update Rollups	Site, AU, SUS, Catalog
Update for Microsoft Security Essentials - 4.4.304.0 (KB2902885)	Critical Updates	Site, AU
Update for Microsoft Security Essentials - 4.4.304.0 (KB2905087)	Critical Updates	Site, AU
Update Rollup 5 for Microsoft System Center Advisor (KB2900542)	Update Rollups	Site, AU, SUS, Catalog
Update for Microsoft Visual Studio 2010 Service Pack 1 (KB2890573)	Critical Updates	Site, AU, SUS, Catalog

Links Públicos de los Boletines de Seguridad Español LATAM

Links de los Boletines en Español

- **Microsoft Security Bulletin Summary for November 2013-Resumo**
  http://technet.microsoft.com/es-es/security/bulletin/ms13-nov
- **Security Bulletin Search/Boletines de Seguradad Busca**
  http://technet.microsoft.com/es-es/security/bulletin
- **Security Advisories/Comunicados de Segurança**
  http://technet.microsoft.com/es-es/security/advisory
- **Microsoft Technical Security Notifications - Notificações**
  http://technet.microsoft.com/es-es/security/dd252948.aspx

Blogs

Seguridad de LATAM

- **http://blogs.technet.com/b/seguridad/**
- MSRC Blog
  http://blogs.technet.com/msrc
- SRD Team Blog
  http://blogs.technet.com/srd
- MMPC Team Blog
  http://blogs.technet.com/mmpc
- MSRC Ecosystem Team Blog
  http://blogs.technet.com/ecostrat

Supplemental Security Reference Articles

- Detailed Bulletin Information Spreadsheet
  http://go.microsoft.com/fwlink/?LinkID=245778
- **Security Tools for IT Pros- Herramientas de Seguridad**
  http://technet.microsoft.com/es-es/security/cc297183
- KB894199 Description of Software Update Services and Windows Server Update Services changes in content
  http://support.microsoft.com/kb/894199
- The Microsoft Windows Malicious Software Removal Tool helps remove specific, prevalent malicious software
  http://support.microsoft.com/kb/890830

Webcast Español DECIEMBRE

Webcast **Español** (Externa)

WEBCAST DE DECIEMBRE - CLIENTES
12/ DECIEMBRE /2013
10:30-11:00 AM - Horário Atlántico

Siga nuestro blog para detalles: Seguridad de LATAM

- **http://blogs.technet.com/b/seguridad**

LATAMSRC@Microsoft.com