Monthly Security Bulletin Briefing - February 2014

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

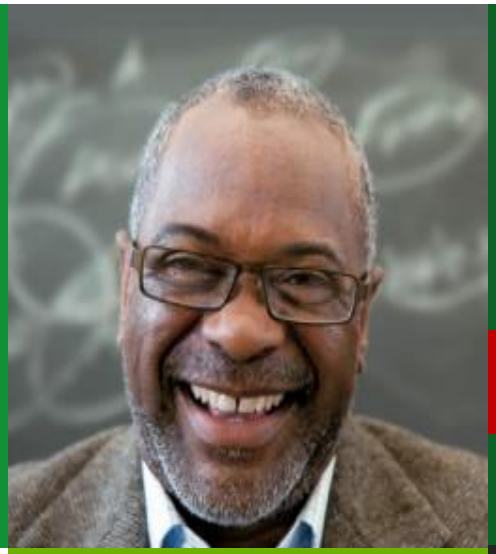
Email: LATAMSRC@Microsoft.com

CSS Security Worldwide Programs

Microsoft

Microsoft

February 2014 Agenda



New Security Bulletins

7

Critical	Important
4	3

1 Security Advisory rerelease

1 Security Advisory revision

Other Security Resources

- ✓ Detection and Deployment Table
- ✓ Product Support Lifecycle Information
- ✓ Public Webcast

CSS Security Worldwide Programs

Microsoft

February 2014 Security Bulletins

Bulletin	Impact	Component	Severity	Priority	Exploit Index	Public
MS14-005	Information Disclosure	MSXML	Important	2	2	Yes
MS14-006	Denial of Service	IPv6	Important	3	3	Yes
MS14-007	Remote Code Execution	Direct2D	Critical	1	1	No
MS14-008	Remote Code Execution	Forefront	Critical	2	1	No
MS14-009	Elevation of Privilege	.NET	Important	2	1	Yes
MS14-010	Remote Code Execution	Internet Explorer	Critical	1	1	Yes
MS14-011	Remote Code Execution	VBScript	Critical	1	1	No

CSS Security Worldwide Programs

Microsoft

MS14-005 Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure (2916036)

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
2	MS10-051 MS12-043 MS13-002	Yes- KB2916036

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	Yes	Yes	Yes

After applying this update, web sites that access data sources across domains may no longer render correctly. See KB2916036 for details.

Note:
Windows RT devices can only be serviced with Windows Update, Microsoft Update, and the Windows Store.

CSS Security Worldwide Programs

MS14-005 Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure (2916036)

Vulnerability Details

- An information disclosure vulnerability exists that could allow an attacker to read files on the local file system of a user, or read content of web domains where a user is currently authenticated. An attacker could exploit this vulnerability when a user views specially crafted web content that is designed to invoke MSXML through Internet Explorer.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2014-0266	Important	Information Disclosure	3	3	*	Yes	Yes	None

Attack Vectors

- A specially crafted website that is designed to invoke MSXML through Internet Explorer.
- Compromised websites and websites that accept or host user-provided content.

Mitigations

- 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.
- Attacker would have to convince users to take action, typically by getting them to click a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by getting them to open an attachment sent through email.

Workarounds

- Prevent MSXML 3.0 binary behaviors from being used in Internet Explorer by setting the kill bit in the registry.
- Set Internet and Local intranet security zone settings to "High."
- Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone.
- Add sites that you trust to the Internet Explorer Trusted sites zone.

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

DoS Rating: **T - Temporary (DoS ends when attack ceases) | P - Permanent (Administrative action required to recover) | * - Not Applicable**

Microsoft

MS14-006 Vulnerability in IPv6 Could Allow Denial of Service (2904659)

Affected Software

- Windows 8
- Windows Server 2012
- Windows RT

Severity | Important

Deployment Priority	Update Replacement	More Information and / or Known Issues
3	MS13-065	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	Yes	Yes	Yes

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

CSS Security Worldwide Programs

Microsoft

MS14-006 Vulnerability in IPv6 Could Allow Denial of Service (2904659)

Vulnerability Details

- A denial of service vulnerability exists in Windows in the IPv6 implementation of TCP/IP. An attacker who successfully exploited this vulnerability could cause the affected system to stop responding.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2014-0254	Important	Denial of Service	NA	3	P	Yes	No	None

Attack Vectors

- An attacker could exploit the vulnerability by creating a large number of specially crafted IPv6 packets and sending the packets to affected systems over a subnet network. The packets could then cause the affected systems to stop responding.

Mitigations

- An attacker's system must belong to the same subnet as the target system.
- Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter.

Workarounds

- Disable the Router Discovery Protocol.
- Disable Internet Protocol version 6 (IPv6).
- Disable the "Core Networking – Router Advertisement (ICMPv6-In)" inbound firewall rule.

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

DoS Rating: **T - Temporary (DoS ends when attack ceases) | P - Permanent (Administrative action required to recover) | * - Not Applicable**

Microsoft

MS14-007 Vulnerability in Direct2D Could Allow Remote Code Execution (2912390)

Affected Software:

- 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	None	Win7/Svr2008 R2 requires 2670838

Restart Requirement

✓ This update may require a restart

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

Platform update for Windows 7 and Server 2008 R2 (KB2670838) is required before applying this update.

Note:
Windows RT devices can only be serviced with Windows Update, Microsoft Update, and the Windows Store.

MS14-007 Vulnerability in Direct2D Could Allow Remote Code Execution (2912390)

Vulnerability Details:

- A remote code execution vulnerability exists in the way that affected Windows components handle specially crafted GIF files. The vulnerability could allow remote code execution if a user views GIF files in shared content. 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-2014-0263	Critical	Remote Code Execution	1	1	*	No	No	None

Attack Vectors

- A specially crafted website that hosts a malicious GIF.
- Compromised websites and websites that accept or host user-provided content.

Mitigations

- Users would have to be persuaded to visit a malicious website.
- Exploitation only gains the same user rights as the logged-on account.

Workarounds

- Microsoft has not identified any workarounds for this vulnerability.

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

DoS Rating: **T - Temporary (DoS ends when attack ceases) | P - Permanent (Administrative action required to recover) | * - Not Applicable**

Microsoft

MS14-008 Vulnerability in Microsoft Forefront Protection for Exchange Could Allow Remote Code Execution (2927022)

Affected Software

- Microsoft Forefront Protection 2010 for Exchange Server

Severity | Critical

Deployment Priority	Update Replacement	More Information and / or Known Issues
2	None	Yes KB2927022

Restart Requirement

✓ May require restart

Uninstall Support

✓ Use Add or Remove Programs in Control Panel

Detection and Deployment

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

Hotfix Rollup 4 for Microsoft Forefront Protection 2010 for Exchange is required to be installed before installing this update.

CSS Security Worldwide Programs

Microsoft

MS14-008 Vulnerability in Microsoft Forefront Protection for Exchange Could Allow Remote Code Execution (2927022)

Vulnerability Details

- A remote code execution vulnerability exists in Forefront Protection for Exchange. An attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the configured service account.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2014-0294	Critical	Remote Code Execution	NA	3	*	No	No	None

Attack Vectors

- An unauthenticated attacker could attempt to exploit this vulnerability by sending a specially crafted email message to an Exchange server that is monitored by affected versions of Forefront Protection for Exchange.

Mitigations

- Microsoft has not identified any mitigations for this vulnerability.

Workarounds

- Microsoft has not identified any workarounds for this vulnerability.

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

DoS Rating: **T - Temporary (DoS ends when attack ceases) | P - Permanent (Administrative action required to recover) | * - Not Applicable**

CSS Security Worldwide Programs

Microsoft

MS14-009 Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2916607)

Affected Software

- Microsoft .NET Framework 1.0 SP3
- Microsoft .NET Framework 1.1 SP1
- Microsoft .NET Framework 2.0 SP2
- Microsoft .NET Framework 3.5
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4
- Microsoft .NET Framework 4.5
- Microsoft .NET Framework 4.5.1

On all supported 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 Server 2012 R2
- Windows RT
- Windows RT 8.1

Detection and Deployment

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

Severity | Important

Deployment Priority	Update Replacement	More Information and / or Known Issues
2	MS11-100 MS13-052	No

Restart Requirement

✓ May require restart

Uninstall Support

✓ Use Add or Remove Programs in Control Panel

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

CSS Security Worldwide Programs

Microsoft

MS14-009 Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2916607)

Vulnerability Details

- CVE-2014-0253: A denial of service vulnerability exists in Microsoft ASP.NET that could allow an attacker to cause an ASP.NET server to become unresponsive.
- CVE-2014-0257: An elevation of privilege vulnerability exists in the Microsoft.NET Framework that could allow an attacker to elevate privileges on the targeted system.
- CVE-2014-0295: A security feature bypass exists in a .NET Framework component that does not properly implement Address Space Layout Randomization (ASLR) that could allow an attacker to bypass the ASLR security feature.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2014-0253	Important	Denial of Service	3	3	P	Yes	No	None
CVE-2014-0257	Important	Elevation of Privilege	1	1	*	No	No	None
CVE-2014-0295	Important	Security Feature Bypass	NA	NA	*	Yes	Yes	None

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

DoS Rating: **T - Temporary (DoS ends when attack ceases) | P - Permanent (Administrative action required to recover) | * - Not Applicable**

MS14-009 Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2916607)

Vulnerability Details (cont'd)

Attack Vectors

CVE-2014-0253 (DoS)

- Specially crafted requests sent to an affected server, causing a denial of service condition.

CVE-2014-0257 (EoP)

- A malicious site could load a specific control allowing the attacker to execute applications on behalf of the user on the targeted system.
- This vulnerability could also be used to exploit .NET Framework applications that expose COM server endpoints.

CVE-2014-0295 (ASLR bypass)

- When a user visits a website that contains malicious content using a web browser capable of instantiating COM components, the affected component can be loaded to bypass ASLR.

Mitigations

CVE-2014-0253 (DoS)

- By default, ASP.NET is not installed on any supported edition of Microsoft Windows.

CVE-2014-0257 and CVE-2014-0295

- Microsoft has not identified any mitigations for these vulnerabilities.

Workarounds

CVE-2014-0253 (DoS)

- Configure the <serverRuntime>, <requestLimits>, and <httpRuntime> elements so that requests that attempt to exploit the vulnerability are rejected.

CVE-2014-0257 (EoP)

- Microsoft has not identified any workarounds for this vulnerability.

CVE-2014-0295 (ASLR bypass)

- Install the Force ASLR feature hotfix and enable the IFEO registry entry. See KB2639308

Microsoft

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

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 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012 R2, and Windows RT 8.1.

Severity | Critical

Deployment Priority	Update Replacement	More Information and / or Known Issues
1	MS13-097	No

Restart Requirement

✓ A restart is required

Uninstall Support

✓ In Control Panel go to Add or Remove Programs

Detection and Deployment

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

On IE9 only this update also addresses the vulnerability in MS14-011 CVE-2014-0271

Note:
Windows RT devices can only be serviced with Windows Update, Microsoft Update, and the Windows Store.

CSS Security Worldwide Programs

Microsoft

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

Vulnerability Details

- CVE-2014-0268: An elevation of privilege vulnerability exists within Internet Explorer during validation of local file installation and during secure creation of registry keys.
- CVE-2014-0271: A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.
- CVE-2014-0293: An information disclosure vulnerability exists in Internet Explorer that could allow an attacker to gain access to information in another domain or Internet Explorer zone. An attacker could exploit the vulnerability by constructing a specially crafted webpage that could allow information disclosure if a user viewed the webpage.
- Multiple: Remote code execution vulnerabilities exist when Internet Explorer improperly accesses objects 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-2014-0268	Important	Elevation of Privilege	3	3	*	No	No	None
CVE-2014-0267	Critical	Remote Code Execution	1	NA	*	Yes	No	None
CVE-2014-0293	Important	Information Disclosure	3	3	*	No	No	None
Multiple	Critical	Remote Code Execution	1 (aggregate)	1 (aggregate)	*	No	No	None

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

DoS Rating: **T - Temporary (DoS ends when attack ceases) | P - Permanent (Administrative action required to recover) | * - Not Applicable**

Microsoft

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

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.

Mitigations

All

Attacker would have to convince users to take action, typically by getting them to click a link in an email message or in an Instant Messenger message that takes users to the attacker's website, or by getting them to open an attachment sent through email. No way for attacker to force user to view malicious content.

CVE-2014-0268 only: This vulnerability by itself does not allow arbitrary code to be run and would have to be used in conjunction with another vulnerability that allowed remote code execution.

All except CVE-2014-0268:

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.

Multiple Memory Corruption CVEs only:

- Exploitation only gains the same user rights as the logged-on account.

Workarounds

All except CVE-2014-0268:

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

CVE-2014-0268 only:

- Microsoft has not identified any workarounds for this vulnerability.

Microsoft

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

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	MS10-022	NA

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	Yes	Yes	Yes

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

CSS Security Worldwide Programs

Microsoft

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

Vulnerability Details

- A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory. The vulnerability may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. If the current user is logged on with administrative user rights, 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-2014-0271	Critical	Remote Code Execution	2	1	*	No	No	None

Attack Vectors

- Specially crafted website.
- An embedded ActiveX control marked "safe for initialization" in an application or Microsoft Office document that hosts the IE rendering engine.
- Compromised websites and websites that accept or host user-provided content or advertisements.

Mitigations

- 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.
- Attacker would have to convince users to take action, typically by getting them to click a link in an email message or in an IM message that takes users to the attacker's website, or by getting them to open an attachment sent through email. No way for attacker to force user to view malicious content.

Workarounds

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

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

DoS Rating: **T - Temporary (DoS ends when attack ceases) | P - Permanent (Administrative action required to recover) | * - Not Applicable**

Microsoft

Rereleased Security Advisory

Security Advisory (2862973)

Update for Deprecation of MD5 Hashing Algorithm for Microsoft Root Certificate Program

As of February 11, 2014, this update is offered via automatic updating and through the Microsoft Update service for all affected software.

Microsoft is announcing the availability of an update for supported editions of Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, and Windows RT that restricts the use of certificates with MD5 hashes. This restriction is limited to certificates issued under roots in the Microsoft root certificate program. Usage of MD5 hash algorithm in certificates could allow an attacker to spoof content, perform phishing attacks, or perform man-in-the-middle attacks.

Revised Security Advisory

Security Advisory (2915720)

Changes in Windows Authenticode Signature Verification

Microsoft is announcing the availability of an update for all supported releases of Microsoft Windows to change how signatures are verified for binaries signed with the Windows Authenticode signature format. The change is included with Security Bulletin MS13-098, but will not be enabled until June 10, 2014. Once enabled, the new default behavior for Windows Authenticode signature verification will no longer allow extraneous information in the WIN_CERTIFICATE structure. Note that after June 10, 2014, Windows will no longer recognize non-compliant binaries as signed.

CSS Security Worldwide Programs

Microsoft

Microsoft Support Lifecycle

Lifecycle Changes

The following product families and service pack levels are scheduled to have their support lifecycle expire on February 11, 2014

Product Family

- No major products this month

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

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

Microsoft

February 2014 Security Bulletins

Bulletin	Description	Severity	Priority
MS14-005	Vulnerability in Microsoft XML Core Services Could Allow Information Disclosure	Important	2
MS14-006	Vulnerability in IPv6 Could Allow Denial of Service	Important	3
MS14-007	Vulnerability in Direct2D Could Allow Remote Code Execution	Critical	1
MS14-008	Vulnerabilities in Microsoft Forefront Protection for Exchange Could Allow Remote Code Execution	Critical	2
MS14-009	Vulnerabilities in .NET Framework Could Allow Elevation of Privilege	Important	2
MS14-010	Cumulative Security Update for Internet Explorer	Critical	1
MS14-011	Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution	Critical	1

CSS Security Worldwide Programs

Appendix

CSS Security Worldwide Programs

Malicious Software Removal Tool (MSRT) Updates

MSRT Changes

New malware families added to the February 2014 MSRT

- VBS/Jenxcus

A family of malware that can be used to take control of PCs and steal sensitive information

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

TechNet Security is Changing!

In 2014 Q1, security bulletins will be moving to the TechNet Library

- Bulletins, bulletin summaries, and advisories will join the existing IT Pro content at http://technet.microsoft.com/library
- TechNet Security portal at http://technet.microsoft.com/security/ will be updated to point to bulletins in the TechNet Library.

Details

- URLs will change from http://technet.microsoft.com/security/bulletin/MSNN-NNN to http://technet.microsoft.com/library/security/MSNN-NNN
- Navigational landing pages will guide gentle readers to the latest bulletins grouped by product family (Windows, IE, .NET, Office, etc.)
- All bulletin content going back to 1998 will be present.

Microsoft

February 2014 Manageability Tools Reference

Bulletin	Windows Update [1]	Microsoft Update [1]	MBSA [2]	WSUS	SMS ITMU	SCCM
MS14-005	Yes	Yes	Yes	Yes	Yes	Yes
MS14-006	Yes	Yes	Yes	Yes	Yes	Yes
MS14-007	Yes	Yes	Yes	Yes	Yes	Yes
MS14-008	No	No	No	No	No	No
MS14-009	Yes	Yes	Yes	Yes	Yes	Yes
MS14-010	Yes	Yes	Yes	Yes	Yes	Yes
MS14-011	Yes	Yes	Yes	Yes	Yes	Yes

1. Windows RT devices can only be serviced with Windows Update, Microsoft Update, and the Windows Store.
2. Microsoft Baseline Security Analyzer (MBSA) v2.3 now supports Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2.

CSS Security Worldwide Programs

February 2014 Non-Security Content

Description	Classification	Deployment
Update for Windows 7 (KB2913751)	Critical Update	Site, AU, SUS, Catalog
Update for Windows 8.1 for x64-based Systems (KB2922474)	Critical Update	Site, AU, SUS, Catalog
Update for Windows RT 8.1 (KB2913760)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft InfoPath 2010 (KB2817369)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft InfoPath 2010 (KB2817396)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft Office 2010 (KB2837583)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft OneNote 2010 (KB2837595)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft Outlook 2010 (KB2687567)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft PowerPoint 2010 (KB2775360)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft SharePoint Workspace 2010 (KB2760601)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft Visio 2010 (KB2817479)	Critical Update	Site, AU, SUS, Catalog
Update for System Center Endpoint Protection 2012 Client - 4.3.215.0 (KB2884678)	Critical Update	Site, AU, SUS, Catalog
Update for System Center Endpoint Protection 2012 Client - 4.4.304.0 (KB2907566)	Critical Update	Site, AU, SUS, Catalog
Update for Forefront Endpoint Protection 2010 Client - 4.3.215.0 (KB2864366)	Critical Update	Site, AU, SUS, Catalog
Update for Forefront Endpoint Protection 2010 Client - 4.4.304.0(KB2907566)	Critical Update	Site, AU, SUS, Catalog

Microsoft

MBSA 2.3

MBSA 2.3 Now Available

The Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations.

MBSA 2.3 release now provides support for Windows 8, Windows 8.1, Windows Server 2012, and Windows Server 2012 R2.

Tool Information

- Available at the Download Center at http://www.microsoft.com/download/details.aspx?id=7558
- Windows 2000 will no longer be supported with this release.

Microsoft

Links Públicos de los Boletines de Seguridad Español LATAM

Links de los Boletines en Español

- **Microsoft Security Bulletin Summary para febrero 2014-Resumo**
  http://technet.microsoft.com/es-es/security/bulletin/ms14-feb
- **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 MARZO

Webcast **Español** (Externo)

WEBCAST - CLIENTES
13/MARZO/2014
10:30-11:15 AM - Horário Atlántico
https://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032575629

Siga nuestro blog para detalles: Seguridad de LATAM

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