Monthly Security Bulletin Briefing (July 2013)

Teresa Ghiorzoe
Security Program Manager LATAM

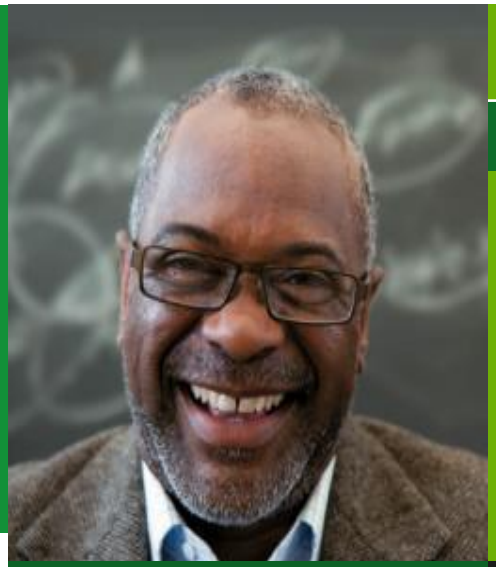
Blog de Seguridad: http://blogs.technet.com/b/seguridad/
Twitter: LATAMSRC

GBS Security Worldwide Programs

Microsoft

Microsoft

July 2013 Agenda



Security Advisories

New	Rerelease
0	1

Other Security Resources

- Detection and Deployment Table

New Security Bulletins

7

Critical	Important
6	1

- Product Support Lifecycle Information
- July 2013 Bulletin Release Summary
- TechNet Public Webcast Details

Appendix

- Malicious Software Removal Tool Updates
- Public Security Bulletin Links
- July 2013 Non-Security Updates

GBS Security Worldwide Programs

Microsoft

July 2013 Security Bulletins

Bulletin	Impact	Component	Severity	Priority	Exploit Index	Public
MS13-052	Remote Code Execution	.NET Framework	Critical	2	1	Yes
MS13-053	Remote Code Execution	Kernel-Mode Drivers	Critical	1	1	Yes
MS13-054	Remote Code Execution	GDI +	Critical	2	1	No
MS13-055	Remote Code Execution	Internet Explorer	Critical	1	1	No
MS13-056	Remote Code Execution	DirectShow	Critical	2	1	No
MS13-057	Remote Code Execution	Media Format Runtime	Critical	2	2	No
MS13-058	Elevation of Privilege	Windows Defender	Important	3	1	No

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

GBS Security Worldwide Programs

Microsoft

MS13-052 Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution (2861561)

Affected Software:

- ✓ .NET Framework 1.0 SP3 on Windows XP Media Center & Tablet PC only
- ✓ .NET Framework 1.1 SP1
- ✓ .NET Framework 2.0 SP2
- ✓ .NET Framework 3.0 SP2
- ✓ .NET Framework 3.5
- ✓ .NET Framework 3.5 SP1
- ✓ .NET Framework 3.5.1
- ✓ .NET Framework 4.0
- ✓ .NET Framework 4.5
  - on all supported editions of Windows
- ✓ Silverlight 5 on Windows (all editions)
- ✓ Silverlight 5 Developer Runtime on Windows
- ✓ Silverlight 5 on Mac
- ✓ Silverlight 5 Developer Runtime on Mac

Detection and Deployment

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

Severity : Critical

Deployment Priority	Update Replacement	More Information and / or Known Issues
2	MS10-060 MS11-078 MS12-034 MS12-035 MS12-074 MS13-004 MS13-022	Yes [3]

Restart Requirement

- ✓ A restart may be required

Uninstall Support

- ✓ Use Add or Remove Programs in Control Panel

1. The MBSA does not support Windows 8, Windows Server 2012, or Windows RT
2. Windows RT devices can only be serviced with Windows and Microsoft Update
3. Windows RT devices require update 2808380 to be installed before WU will offer this security update

GBS Security Worldwide Programs

Microsoft

MS13-052 Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution (2861561)

Vulnerability Details:

- Four (4) remote code execution vulnerabilities exist in the .NET Framework and Silverlight that could allow an attacker to take complete control of an affected system if a user can be convinced to view a website that contains a specially crafted Silverlight application or to run a specially crafted Windows .NET Framework application.
- Three (3) elevation of privilege vulnerabilities exist in the .NET Framework that could allow an attacker to take complete control of an affected system if a user can be convinced to view a website and run a specially crafted XBAP (XAML browser application) or to run a Windows .NET Framework application.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-3129	Critical	Remote Code Execution	1	1	P	No	None	None
CVE-2013-3131	Critical	Remote Code Execution	2	2	NA	**Yes**	None	None
CVE-2013-3132	Important	Elevation of Privilege	3	3	NA	No	None	None
CVE-2013-3133	Important	Elevation of Privilege	3	3	NA	No	None	None
CVE-2013-3134	Critical	Remote Code Execution	2	2	NA	**Yes**	None	None
CVE-2013-3171	Important	Elevation of Privilege	3	3	NA	No	None	None
CVE-2013-3178	Critical	Remote Code Execution	1	1	NA	No	None	None

Attack Vectors

- A specially crafted Web page
- A specially crafted XAML browser application
- A specially crafted Windows .NET application
- A specially crafted Silverlight application
- A specially crafted TrueType font file for CVE-2013-3129

Mitigations

- Exploitation only gains the same user rights as the logged on account
- Users would have to be persuaded to visit a malicious web site
- Cannot be exploited automatically through e-mail, because a user must open an attachment
- By default, XBAP applications prompt the user before executing code
- By default, IE runs in a restricted mode for all Windows Servers
- There are no mitigations for CVE-2013-3129, CVE-2013-3171

Workarounds

- Disable Silverlight in IE, Firefox, or Chrome for CVE-2013-3131 and CVE-2013-3178
- Disable partially trusted .NET apps for CVE-2013-3131
- Disable XAML browser apps in IE
- Restrict websites to only your trusted websites
- There are no workarounds for CVE-2013-3129, CVE-2013-3134, and CVE-2013-3171

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)

GBS Security Worldwide Programs

Microsoft

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

Affected Software:

- ✓ Windows XP (all editions)
- ✓ Windows Server 2003 (all editions)
- ✓ Windows Vista (all editions)
- ✓ Windows Server 2008 (all editions)
- ✓ Windows 7 (all editions)
- ✓ Windows Server 2008 R2 (all editions)
- ✓ Windows 8 (all editions)
- ✓ Windows Server 2012 (all editions)
- ✓ Windows RT (all editions)

Severity | Critical

Deployment Priority	Update Replacement	More Information and / or Known Issues
1	MS13-036 MS13-046	Yes [3]

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 MBSA does not support Windows 8, Windows Server 2012, or Windows RT
2. Windows RT devices can only be serviced with Windows and Microsoft Update
3. Windows RT devices require update 2808380 to be installed before WU will offer this security update

GBS Security Worldwide Programs

Microsoft

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

Vulnerability Details:

- Two (2) remote code execution vulnerabilities exist in the way that the Windows kernel-mode drivers improperly handle objects in memory and specially crafted TrueType font files could allow an attacker to take complete control of an affected system if a user opens a specially crafted file.
- Five (5) elevation of privilege vulnerabilities exist when the Windows kernel-mode drivers improperly handle objects in memory that could allow an attacker to execute arbitrary code with elevated privileges.
- A denial of service vulnerability exists in the way that the Windows kernel-mode driver improperly handles objects in memory that could allow an attacker to cause the target system to stop responding.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-1300	Important	Elevation of Privilege	1	1	P	No	No	None
CVE-2013-1340	Important	Elevation of Privilege	3	1	P	No	No	None
CVE-2013-1345	Important	Elevation of Privilege	3	1	P	No	No	None
CVE-2013-3129	Critical	Remote Code Execution	1	1	P	No	No	None
CVE-2013-3167	Important	Elevation of Privilege	NA	1	P	No	No	None
CVE-2013-3172	Moderate	Denial of Service	*	*	P	**Yes**	No	None
CVE-2013-3173	Important	Elevation of Privilege	1	1	P	No	No	None
CVE-2013-3660	Critical	Remote Code Execution	3	3	P	**Yes**	**Yes**	None

Attack Vectors

- A specially crafted application
- A specially crafted TrueType font file for CVE-2013-3129

Mitigations

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

For CVE-2013-3129

- Users would have to be persuaded to visit a malicious web site
- Cannot be exploited automatically through e-mail, because a user must open an attachment
- By default, all Microsoft e-mail clients open HTML e-mail messages in the Restricted Sites zone

Workarounds

- Microsoft has not identified any workarounds for any of these vulnerabilities except...

For CVE-2013-3129

- Disable the WebClient service
- Block TCP ports 139 and 445 at the firewall
- Disable the Preview Pane and Details Pane in Windows 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

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

Affected Software:

- ✓ Windows XP (all editions)
- ✓ Windows Server 2003 (all editions)
- ✓ Windows Vista (all editions)
- ✓ Windows Server 2008 (all editions)
- ✓ Windows 7 (all editions)
- ✓ Windows Server 2008 R2 (all editions)
- ✓ Windows 8 (all editions)
- ✓ Windows Server 2012 (all editions)
- ✓ Windows RT (all editions)
- ✓ Office 2003 (all editions)
- ✓ Office 2007 (all editions)
- ✓ Office 2010 (all editions)
- ✓ Visual Studio .NET 2003 SP1 [3]
- ✓ Lync 2010, Lync 2010 Attendee, Lync 2013, and Lync Basic 2013

Detection and Deployment

WU	MU	MBSA	WSUS	ITMU	SCCM
Yes [3]	Yes	Yes [1 | 2]	Yes [2]	Yes [2]	Yes [2]

Severity | Critical

Deployment Priority	Update Replacement	More Information and / or Known Issues
2	MS09-062 MS12-034 MS13-041	Yes [4]

Restart Requirement

- ✓ A restart may be required

Uninstall Support

- ✓ Use Add or Remove Programs in Control Panel

1. The MBSA does not support Windows 8, Windows Server 2012, or Windows RT
2. Windows RT devices can only be serviced with Windows and Microsoft Update
3. Office and Lync are not supported by Windows Update, and the Visual Studio update is only available from the Download Center
4. MU or WU may offer this update even though you do not have an Office 2003 application

GBS Security Worldwide Programs

Microsoft

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

Vulnerability Details:

A remote code execution vulnerability exists in the way that affected Windows components and other affected software handle specially crafted TrueType font files. The vulnerability could allow an attacker to take complete control of an affected system if a user opens or previews a file or website containing a specially crafted TrueType Font (TTF) file with an affected version of Microsoft software

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-3129	Critical	Remote Code Execution	1	1	P	No	None	None

Attack Vectors

- A maliciously crafted TrueType font file
- Common delivery mechanisms: a maliciously crafted Web page, an e-mail attachment, an instant message, a peer-to-peer file share, a network share, and/or a USB thumb drive

Mitigations

- Users would have to be persuaded to visit a malicious web site
- Cannot be exploited automatically through e-mail, because a user must open an attachment
- By default, all Microsoft e-mail clients open HTML e-mail messages in the Restricted Sites zone

Workarounds

- Disable the WebClient service
- Block inbound TCP ports 139 and 445 at the firewall
- Disable the Preview Pane and Details Pane in Windows 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)

Note that the TrueType Font Parsing Vulnerability (CVE-2013-3129) also affects the following products:

- ✓ .NET Framework (MS13-052)
- ✓ Silverlight (MS13-052)
- ✓ Windows Kernel-Mode Driver (MS13-053)
- ✓ Windows components (MS13-054)
- ✓ Office (MS13-054)
- ✓ Lync (MS13-054)
- ✓ Visual Studio (MS13-054)

You need to install only the updates that correspond to the software you have installed on your system. If you need to install more than one of these updates, they can be installed in any sequence.

GBS Security Worldwide Programs

Microsoft

MS13-055 Cumulative Security Update for Internet Explorer (2846071)

Affected Software:

- ✓ IE 6 on Windows XP and Windows Server 2003
- ✓ IE 7 on Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008
- ✓ IE 8 on Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2
- ✓ IE 9 on Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2
- ✓ IE 10 on Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, and Windows RT

Detection and Deployment

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

Severity | Critical

Deployment Priority	Update Replacement	More Information and / or Known Issues
1	MS13-047	Yes [3]

Restart Requirement

- ✓ A restart is required

Uninstall Support

- ✓ Use Add or Remove Programs in Control Panel

1. The MBSA does not support Windows 8, Windows Server 2012, or Windows RT
2. Windows RT devices can only be serviced with Windows and Microsoft Update
3. Windows RT devices require update 2808380 to be installed before WU will offer this security update

GBS Security Worldwide Programs

Microsoft

MS13-055 Cumulative Security Update for Internet Explorer (2846071)

Vulnerability Details:

- Sixteen (16) remote code execution vulnerabilities exist in the way that Internet Explorer accesses an object in memory that has been deleted. These vulnerabilities could allow an attacker to take complete control of an affected system if they can convince a user to view a specially crafted website, a compromised website, or a website that accepts or hosts user-provided content or advertisements.
- A cross-site-scripting (XSS) vulnerability exists in Internet Explorer that could allow an attacker to gain access to information in another domain or Internet Explorer zone.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
Multiple * CVE-2013-3166	Critical Important	Remote Code Execution Information Disclosure	1 3	1 3	NA NA	No No	No No	None None

Attack Vectors

- A maliciously crafted Web page
- Compromised websites and websites that accept or host user-provided content or advertisements

* CVE-2013-3115 CVE-2013-3143 CVE-2013-3144 CVE-2013-3145 CVE-2013-3146 CVE-2013-3147 CVE-2013-3148 CVE-2013-3149 CVE-2013-3150 CVE-2013-3151 CVE-2013-3152 CVE-2013-3153 CVE-2013-3161 CVE-2013-3162 CVE-2013-3163 CVE-2013-3164

Mitigations

- Users would have to be persuaded to visit a malicious web site
- Exploitation only gains the same user rights as the logged on account
- By default, all Microsoft e-mail clients open HTML e-mail messages in the Restricted Sites zone
- By default, IE runs in a restricted mode for all Windows Servers

Workarounds

- Set IE security to High for Internet and Intranet zones
- Configure IE to prompt before running ActiveX and Active Scripting

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

MS13-056 Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (2845187)

Affected Software:

- ✓ Windows XP (all editions)
- ✓ Windows Server 2003 (all editions)
- ✓ Windows Vista (all editions)
- ✓ Windows Server 2008 for 32-bit Systems SP2
- ✓ Windows Server 2008 for 64-bit Systems SP2
- ✓ Windows 7 (all editions)
- ✓ Windows Server 2008 R2 for 64-bit Systems SP1
- ✓ Windows 8 (all editions)

Detection and Deployment

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

Severity | Critical

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

Restart Requirement

- ✓ A restart may be required

Uninstall Support

- ✓ Use Add or Remove Programs in Control Panel

Server Core installations of Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 are not affected by this issue

GBS Security Worldwide Programs

MS13-056 Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (2845187)

Vulnerability Details:

A remote code execution vulnerability exists in the way that Microsoft DirectShow parses GIF image files that could allow an attacker to take complete control of an affected system if a user can be persuaded to open a specially crafted GIF file.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-3174	Critical	Remote Code Execution	1	1	T	No	None	None

Attack Vectors

- A maliciously crafted .GIF file
- Common delivery mechanisms: a maliciously crafted Web page, an e-mail attachment, an instant message, a peer-to-peer file share, a network share, and/or a USB thumb drive

Mitigations

- Users would have to be persuaded to visit a malicious web site
- Exploitation only gains the same user rights as the logged on account
- Cannot be exploited automatically through e-mail, because a user must open an attachment

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

MS13-057 Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution (2847883)

Affected Software:

- ✓ Windows Media Format Runtime 9
- ✓ Windows Media Format Runtime 9.5
- ✓ Windows Media Format Runtime 9.5 x64
- ✓ Windows Media Format Runtime 11
- ✓ Windows Media Player 11
- ✓ Windows Media Player 12
- on all supported editions of Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, and Windows RT

Detection and Deployment

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

Severity | Critical

Deployment Priority	Update Replacement	More Information and / or Known Issues
2	None	Yes [3]

Restart Requirement

- ✓ A restart may be required

Uninstall Support

- ✓ Use Add or Remove Programs in Control Panel

1. The MBSA does not support Windows 8, Windows Server 2012, or Windows RT
2. Windows RT devices can only be serviced with Windows and Microsoft Update
3. Windows RT devices require update 2808380 to be installed before WU will offer this security update

GBS Security Worldwide Programs

MS13-057 Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution (2847883)

Vulnerability Details:

A remote code execution vulnerability exists in the way Windows Media Format Runtime handles certain media files that could allow an attacker to take complete control of an affected system if a user can be persuaded to open a specially crafted media file

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-3127	Critical	Remote Code Execution	2	2	T	No	None	None

Attack Vectors

- A maliciously crafted Media file
- Common delivery mechanisms: a maliciously crafted Web page, an e-mail attachment, an instant message, a peer-to-peer file share, a network share, and/or a USB thumb drive

Mitigations

- Users would have to be persuaded to visit a malicious web site
- Exploitation only gains the same user rights as the logged on account
- Cannot be exploited automatically through e-mail, because a user must open an attachment

Workarounds

- Un-register Wmp.dll

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

MS13-058 Vulnerability in Windows Defender Could Allow Elevation of Privilege (2847927)

Affected Software:

- ✓ Windows Defender for Windows 7 (x86)
- ✓ Windows Defender for Windows 7 (x64)
- ✓ Windows Defender on Windows Server 2008 R2 (x64)

Severity | Important

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

Restart Requirement

- ✓ A restart is not 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

- If Windows Defender is disabled, you do not need to install this update
- Windows Defender is included with the Desktop Experience feature for Windows Server 2008 R2

GBS Security Worldwide Programs

MS13-058 Vulnerability in Windows Defender Could Allow Elevation of Privilege (2847927)

Vulnerability Details:

An elevation of privilege vulnerability exists when improper pathnames are used by affected versions of Windows Defender. The vulnerability could allow an attacker with valid logon credentials to log on locally and run arbitrary code in the context of the LocalSystem and take complete control of the system by placing a specially crafted application in a location that could be used to exploit the vulnerability.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2013-3176	Important	Elevation of Privilege	NA	1	NA	No	No	None

Attack Vectors

- A maliciously crafted application

Mitigations

- An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability
- Windows 7 standard user accounts do not have permissions to write files to the root directory by default

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

Security Advisory Rerelease

Security Advisory (2755801)

Update for Vulnerabilities in Adobe Flash Player in Internet Explorer 10

- ✓ Windows 8 for 32-bit and 64-bit Systems
- ✓ Windows Server 2012
- ✓ Windows RT

Reason for rerelease:

- ✓ The update addresses the vulnerabilities described in Adobe Security bulletin APSB13-17
- ✓ For more information about this update, including download links, see KB Article 2857645

Also note

- ✓ This update is also available for the IE 11 Preview in Windows 8.1 Preview and Windows 8.1 RT Preview releases

GBS Security Worldwide Programs

Microsoft

July 2013 Manageability Tools Reference

Bulletin	Windows Update	Microsoft Update	MBSA	WSUS	SMS ITMU	SCCM
MS13-052 [4]	Yes	Yes	Yes [1] [2]	Yes [2]	Yes [2]	Yes [2]
MS13-053	Yes	Yes	Yes [1] [2]	Yes [2]	Yes [2]	Yes [2]
MS13-054	Yes [3]	Yes	Yes [1]	Yes	Yes	Yes
MS13-055	Yes	Yes	Yes [1] [2]	Yes [2]	Yes [2]	Yes [2]
MS13-056	Yes	Yes	Yes [1]	Yes	Yes	Yes
MS13-057	Yes	Yes	Yes [1] [2]	Yes [2]	Yes [2]	Yes [2]
MS13-058	Yes	Yes	Yes	Yes	Yes	Yes

1. The MBSA does not support detection on Windows 8, Windows Server 2012, or Windows RT systems
2. Windows RT devices can only be serviced with Windows and Microsoft Update and the Microsoft Store
3. Office and Lync are not supported by Windows Update, and the Visual Studio update is only available from the Download Center
4. Silverlight on Mac is not supported by any of our standard automatic deployment mechanisms, but they do include a self-update feature

GBS 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 July 9th 2013

Product Family

- Commerce Server 2002 Enterprise Edition
- Commerce Server 2002 Standard Edition
- Windows CE .NET 4.2
- Visual J# .NET Version 1.1 Redistributable Package

Service Pack Level

- Search Server 2008
- Search Server 2008 Express
- System Center Mobile Device Manager 2008
- Windows Web Server 2008
- Windows Web Server 2008 R2
- Dynamics GP 2010 Service Pack 1
- Dynamics SL 7.0 Service Pack 3
- Office for Mac 2011 Service Pack 1

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

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

GBS Security Worldwide Programs

Microsoft

July 2013 Security Bulletins

Bulletin	Description	Severity	Priority
MS13-052	Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution	Critical	2
MS13-053	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution	Critical	1
MS13-054	Vulnerability in GDI+ Could Allow Remote Code Execution	Critical	2
MS13-055	Cumulative Security Update for Internet Explorer	Critical	1
MS13-056	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution	Critical	2
MS13-057	Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution	Critical	2
MS13-058	Vulnerability in Windows Defender Could Allow Elevation of Privilege	Important	3

GBS Security Worldwide Programs

Appendix

GBS Security Worldwide Programs

Malicious Software Removal Tool Updates (MSRT)

MSRT Changes

No new malware families are being added to the July tool

- A phased deployment plan is being used to progressively rollout out MSRT v5 to the install base while verifying its quality.
- On July 9th the MSRT will be made available on the Download Center and to users who select the tool on Microsoft Update
- The new version will allow MSRT to adopt new engine features faster and with less risk/effort

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

July 2013 Non- Security Content (Windows)

Description	Classification	Deployment
Update for Windows 8.1 Preview (KB2863147)	Update (Recommended)	Site, AU
Update for Windows 8.1 Preview (KB2866512)	Update (Recommended)	Site, AU
Update for Windows 8.1 Preview (KB2866518)	Update (Recommended)	Site, AU
Update for Windows 8.1 Preview (KB2865946)	Update (Recommended)	Site, AU
Update for Windows 8.1 Preview (KB2866763)	Update (Recommended)	Site, AU
Update for Microsoft Camera Codec Pack for Windows 8 (KB2859541)	Update (Recommended)	Site, AU, SUS, Catalog
Update for Windows 7 (KB2574819)	Update (Recommended)	Site, AU, SUS, Catalog
Update for Windows 7 (KB2829104)	Update	Catalog
Update for Microsoft .NET Framework 2.0 SP2 on Windows Server 2008 SP2 x86 (KB2836945)	Update (Recommended)	Site, AU, SUS, Catalog
Update for Windows 8 (KB2802618)	Critical Update	Site, AU, SUS, Catalog
Update for Windows 8 (KB2855336)	Critical Update	Site, AU, SUS, Catalog
Windows Malicious Software Removal Tool for Windows 8 - July 2013 (KB890830)	Update Rollup	Site, AU, SUS, Catalog

Microsoft

July 2013 Non- Security Content

(Office, Exchange, and Dynamics CRM)

Description	Classification	Deployment
Update for Microsoft Word 2013 (KB2810086)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft Word 2013 (KB2767863)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft SharePoint Enterprise Server 2013 (KB2817321)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft Office 2013 (KB2767851)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft Outlook 2013 (KB2817468)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft OneNote 2013 (KB2817467)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft PowerPoint 2013 (KB2810006)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft Office 2013 (KB2817482)	Critical Update	Site, AU, SUS, Catalog
Update for Outlook 2003 Junk E-mail Filter (KB2817523)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft Office 2013 (KB2817489)	Critical Update	Site, AU, SUS, Catalog
Definition Update for Microsoft Office 2013 (KB2760587)	Definition Update	Site, AU, SUS, Catalog
Update for Microsoft Office 2013 (KB2817492)	Critical Update	Site, AU, SUS, Catalog
Update for Microsoft Office Outlook 2007 Junk Email Filter (KB2817563)	Critical Update	Site, AU, SUS, Catalog
Update Rollup 1 for Exchange Server 2010 Service Pack 3 (KB2803727)	Update Rollup	Site, AU, SUS, Catalog
Update Rollup 14 for Microsoft Dynamics CRM 2011	Update Rollup	Site, AU, SUS, Catalog

Public Security Bulletin Links

Monthly Bulletin Links

- Microsoft Security Bulletin Summary for July 2013
  http://technet.microsoft.com/en-us/security/bulletin/ms13-jul
- Security Bulletin Search
  http://technet.microsoft.com/en-us/security/bulletin
- Security Advisories
  http://technet.microsoft.com/en-us/security/advisory
- Microsoft Technical Security Notifications
  http://technet.microsoft.com/en-us/security/dd252948.aspx

Blogs

- 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
  http://technet.microsoft.com/en-us/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

Public Webcast August 2013

Webcast Spanish Customers

ESPAÑOL (límite de 250 personas por orden de llegada)

Fecha: Jueves, 15 de Agosto de 2013, 10:00-10:30 hora del Atlántico (Eastern/Miami)

Spanish Blog & Twitter

Security Blog in Spanish
http://blogs.technet.com/b/seguridad/
Twitter: LATAMSRC

GBS Security Worldwide Programs