Monthly Security Bulletin Briefing

March 2014

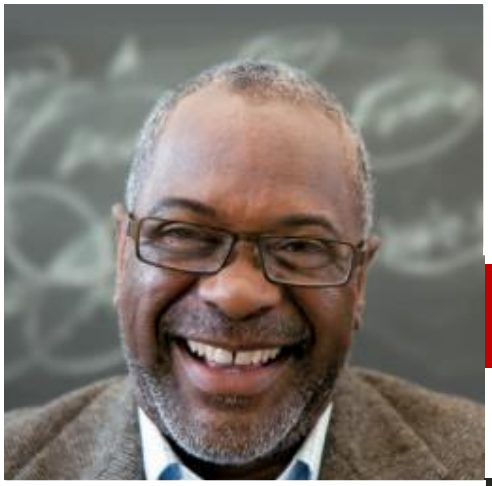
- **Teresa Ghiorzoe**
  Security Program Manager- GBS LATAM
- **Daniel Mauser**
  Senior Technical Lead - LATAM CTS

Blog de Segurança: http://blogs.technet.com/b/risco/

Twitter: LATAMSRC

Email: LATAMSRC@Microsoft.com

March 2014 | Security Bulletin Release Overview



New Security Bulletins **5**

Critical	Important
2	3

Security Advisory Rerelease **1**

Other content

- Product Support Lifecycle
- Manageability Tools Reference

Appendix

- Public Webcast Details
- Related Resources

March 2014 | Security Bulletin Release Overview

Bulletin	Impact	Component	Severity	Priority	Exploit Index	Publicly Known	Publicly Exploited
MS14-012	Remote Code Execution	IE	Critical	**1**	1	Yes	Yes
MS14-013	Remote Code Execution	DirectShow	Critical	2	3	No	No
MS14-014	Security Feature Bypass	Silverlight	Important	2	NA	No	No
MS14-015	Elevation of Privilege	KMD	Important	2	1	Yes	No
MS14-016	Security Feature Bypass	SAMR	Important	3	NA	No	No

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

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	MS14-010	Yes

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 8.1 and Windows Server 2012 R2 require KB2904440

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

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

Vulnerability Details

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

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
Multiple	Critical	Remote Code Execution	1	1	*	Yes	Yes	2934088

Attack Vectors

- An attacker could host a specially crafted website that is designed to exploit this vulnerability through IE and then convince a user to view the website. Attack website can include 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.
- By default, all Microsoft email clients open HTML email messages in the Restricted Sites zone.
- By default, Internet Explorer runs in a restricted mode for all Windows Servers.

Workarounds

- Apply the Microsoft Fix it solution, "MSHTML Shim Workaround," that prevents exploitation of CVE-2014-0322.
- 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.

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**

MS14-013 | Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (2929961)

Affected Software

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008 (except Itanium)
- Windows 7
- Windows Server 2008 R2 (except Itanium)
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2

Severity | Critical

Deployment Priority	Update Replacement	More Information and / or Known Issues
2	MS13-056	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
Yes	Yes	Yes	Yes	Yes	Yes

Servers not affected unless Desktop Experience is enabled (except Server 2003)

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

MS14-013 | Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (2929961)

Vulnerability Details

- A remote code execution vulnerability exists in the way that Microsoft DirectShow parses specially crafted JPEG image files. The vulnerability could allow remote code execution if a user opens a specially crafted image file.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2014-0301	Critical	Remote Code Execution	3	3	*	No	No	None

Attack Vectors

- An attacker could host a website that contains specially crafted content that is used to attempt to exploit this vulnerability.
- An attacker could exploit the vulnerability by sending a specially crafted JPEG file as a email attachment and by convincing the user to open the file.

Mitigations

- In a web-based attack scenario, an 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 message that takes users to the attacker's website, or by opening an attachment sent through email.
- For an email based attack to be successful, a user must open an attachment that is sent in an email message.
- Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

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**

MS14-014 | Vulnerability in Silverlight Could Allow Security Feature Bypass (2932677)

Affected Software:

- Silverlight 5 when installed on Mac.
- Silverlight 5 Developer Runtime when installed on Mac.
- Silverlight 5 when installed on Windows clients.
- Silverlight 5 Developer Runtime when installed on Windows clients.
- Silverlight 5 when installed on Windows servers.
- Silverlight 5 Developer Runtime when installed on Windows servers.

Severity | Important

Deployment Priority	Update Replacement	More Information and / or Known Issues
2	MS13-087	KB2939344

Restart Requirement

- A restart may be required.

Uninstall Support

- Windows: Add or Remove Programs Control Panel applet (must remove Silverlight to install update).
- Mac: Open the Finder, select the system drive, go to the folder Internet Plug-ins - Library, and delete the file Silverlight.Plugin (must remove Silverlight to install update).

Detection and Deployment

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

Silverlight now supports Enhanced Protected Mode (EPM) in Internet Explorer 11 in Windows 8.1

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

MS14-014 | Vulnerability in Silverlight Could Allow Security Feature Bypass (2932677)

Vulnerability Details:

- A security feature vulnerability exists in Silverlight due to improper implementation of Data Execution Protection (DEP) and Address Space Layout Randomization (ASLR). The vulnerability could allow an attacker to bypass the DEP/ASLR security feature, most likely during or in the course of exploiting a remote code execution vulnerability.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2014-0319	Important	Security Feature Bypass	NA	NA	*	No	No	None

Attack Vectors

- An attacker could host a specially crafted website with Silverlight content that is designed to exploit this vulnerability through the web browser and then convince a user to view the website. Attack website can include websites that accept or host user-provided content.

Mitigations

- Users would have to be persuaded to visit a malicious website, typically by getting them to click a link in an email message or instant message that takes users to the attacker's website.
- Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.
- By default, Internet Explorer runs in a restricted mode on all Windows Servers.

Workarounds

- Temporarily prevent Microsoft Silverlight from running in Internet Explorer.
- Temporarily prevent Microsoft Silverlight from running in Mozilla Firefox.
- Temporarily prevent Microsoft Silverlight from running in Google Chrome.

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**

MS14-015 | Vulnerabilities in Windows Kernel Mode Driver Could Allow Elevation of Privilege (2930275)

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	MS13-101 MS14-003	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

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

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

MS14-015 | Vulnerabilities in Windows Kernel Mode Driver Could Allow Elevation of Privilege (2930275)

Vulnerability Details

- An elevation of privilege vulnerability (CVE-2014-0300) exists when the Windows kernel-mode driver improperly handles objects in memory. An attacker who successfully exploited this vulnerability could gain elevated privileges and read arbitrary amounts of kernel memory.
- An information disclosure vulnerability (CVE-2014-0323) exists in the way that the Windows kernel-mode driver improperly handles objects in memory.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2014-0300	Important	Elevation of Privilege	1	1	P	No	No	None
CVE-2014-0323	Important	Information Disclosure	3	3	P	Yes	No	No

Attack Vector

- An attacker would first have to log on to the system and then run a specially crafted application.

Mitigations

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

Workarounds

- Microsoft has not identified any workarounds for these vulnerabilities.

MS14-016 | Vulnerability in Security Account Manager Remote (SAMR) Protocol Could Allow Security Feature Bypass (2934418)

Affected Software

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Severity | Important

Deployment Priority	Update Replacement	More Information and / or Known Issues
3	MS11-095 MS13-032	None

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

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

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

MS14-016 | Vulnerability in Security Account Manager Remote (SAMR) Protocol Could Allow Security Feature Bypass (2934418)

Vulnerability Details

- A security feature bypass vulnerability exists when the Security Account Manager Remote (SAMR) protocol incorrectly validates user lockout state. An attacker who successfully exploited this vulnerability could conduct brute force attacks against user passwords.

CVE	Severity	Impact	XI Latest	XI Legacy	XI DoS	Public	Exploited	Advisory
CVE-2014-0317	Important	Security Feature Bypass	*	*	*	No	No	None

Attack Vectors

- An attacker would need a user name and must be on the same virtual local area network as the target system.

Mitigations

- Microsoft has not identified any mitigating factors 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**

Rereleased Security Advisory

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

What Has Changed?	Microsoft updated this advisory to announce the availability of a new update for Adobe Flash Player. On March 11, 2014, Microsoft released an update (KB2916626) for all supported editions of Windows 8, Windows 8.1, Windows Server 2012, Windows Server 2012 R2, and Windows RT. The update addresses the vulnerabilities described in Adobe Security bulletin APSB14-08. For more information about this update, including download links, see Microsoft Knowledge Base Article 2916626.
Executive Summary	Microsoft is announcing the availability of an update for Adobe Flash Player in Internet Explorer on all supported editions of Windows 8, Windows Server 2012, Windows RT, Windows 8.1, Windows Server 2012 R2, and Windows RT 8.1. The update addresses the vulnerabilities in Adobe Flash Player by updating the affected Adobe Flash libraries contained within Internet Explorer 10 and Internet Explorer 11.
Recommendations	Microsoft recommends that customers apply the current update immediately using update management software, or by checking for updates using the Microsoft Update service. Since the update is cumulative, only the current update will be offered. Customers do not need to install previous updates as a prerequisite for installing the current update.
More Information	http://technet.microsoft.com/security/advisory/2755801

Support Lifecycle

Product Families and Service Packs Reaching End of Support

Product Families	No product families are scheduled to have their support lifecycle expire on March 11, 2014
Service Packs	No service packs are scheduled to have their support lifecycle expire on March 11, 2014
Windows XP	Remember that support for the entire Windows XP product family will expire on 4/8/2014
More Information	http://support.microsoft.com/lifecycle

March 2014 | Detection & Deployment (Manageability Tools) Reference

Bulletin	Windows Update [1]	Microsoft Update [1]	MBSA [2]	WSUS	SMS ITMU	SCCM
MS14-012	Yes	Yes	Yes	Yes	Yes	Yes
MS14-013	Yes	Yes	Yes	Yes	Yes	Yes
MS14-014	Yes	Yes	Yes	Yes	Yes	Yes
MS14-015	Yes	Yes	Yes	Yes	Yes	Yes
MS14-016	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.

March 2014 | Security Bulletin Summary

Bulletin	Bulletin title	Severity	Priority
MS14-012	Cumulative Security Update for Internet Explorer	Critical	1
MS14-013	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution	Critical	2
MS14-014	Vulnerability in Silverlight Could Allow Security Feature Bypass	Important	2
MS14-015	Vulnerabilities in Windows Kernel Mode Driver Could Allow Elevation of Privilege	Important	2
MS14-016	Vulnerability in Security Account Manager Remote (SAMR) Protocol Could Allow Security Feature Bypass	Important	3

Appendix

CSS Security Worldwide Programs

Related Resources

MSRT Changes, Tools, and Public Security Bulletin Webcast

Malicious Software Removal Tool (MSRT)	Win32/Wysotot - A family of malware that can change the browser start page. Win32/Spacekito - A family of malware that downloads and installs plugins for Internet Explorer, Firefox, and Chrome.
Additional Malware Removal 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
Public Webcast	Information About Microsoft's Security Bulletins Wednesday, March 12, 2014, 11:00 A.M. Pacific Time (US & Canada) Register at: https://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032572977
Microsoft Security Blogs	Microsoft Security Response Center Blog: http://blogs.technet.com/msrc Microsoft Security Research Defense Blog: http://blogs.technet.com/srd Microsoft Malware Protection Center Blog: http://blogs.technet.com/mmpc Microsoft Security Development Lifecycle Blog: http://blogs.technet.com/sdl

March 2014 | Windows Non-Security Content

Update	Classification	Deployment	Platform
Windows Malicious Software Removal Tool – March 2014 (KB890830)	Update Rollup	Site,AU,SUS,Catalog	All
Dynamic Update for Windows 8.1 (KB2920540)	Critical Update	Site, AU	Win8.1/Win2k12R2
Update for Windows 8.1 (KB2919442)	Critical Update	Site, AU, SUS, Catalog	Win8.1/Win2k12R2
Update for Windows 8.1 (KB2928680)	Critical Update	Site, AU, SUS, Catalog	Win8.1/Win2k12R2
Update for Windows 7 (KB2929733)	Critical Update	Site, AU, SUS, Catalog	Vista/Win7/Win2k8/Win2k8R2
Dynamic Update for Windows 8.1 (KB2930294)	Critical Update	Site, AU, SUS	Win8.1
Dynamic Update for Windows 8.1 (KB2930168)	Critical Update	Site, AU, SUS	Win8.1/Win2k12R2
Dynamic Update for Windows 8.1 (KB2930169)	Critical Update	Site, AU, SUS	Win8.1/Win2k12R2
Update for Windows 8.1 (KB2913760)	Critical Update	Site, AU, SUS, Catalog	Win8.1/Win2k12R2

Links Públicos dos Boletin de Segurança Português LATAM

Links do Boletins em Português

- **Microsoft Security Bulletin Summary for March 2014- Resumo**
  http://technet.microsoft.com/pt-br/security/bulletin/ms14-Mar
- **Security Bulletin Search/Boletins de Segurança Busca**
  http://technet.microsoft.com/pt-br/security/bulletin
- **Security Advisories/Comunicados de Segurança**
  http://technet.microsoft.com/pt-br/security/advisory
- **Microsoft Technical Security Notifications - Notificações**
  http://technet.microsoft.com/pt-br/security/dd252948.aspx

Blogs

Negócios de Risco

- **http://blogs.technet.com/b/risco/**
- 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- Ferramentas de Segurança**
  http://technet.microsoft.com/pt-br/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 Português Abril

Webcast Português (Externo)

WEBCAST – CLIENTES

https://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032575581

10/ Abril/2014

15:30 Hrs Brasília

Para receber convite para a conferência escrever para LATAMSRC@Microsoft.com