



eSecurity Advisory JANUARY 2013 MICROSOFT SECURITY BULLETIN RELEASE

The purpose of this update is to provide you with a summary of the Microsoft January 2013 Security Bulletin release.

NEW BULLETINS

Microsoft released the following security bulletins for newly discovered vulnerabilities:

Severity	Bulletin ID	Affected Product	Impact
Critical	MS13-001	Microsoft Windows	Remote Code Execution
Critical	MS13-002	Microsoft Windows	Remote Code Execution
Important	MS13-003	System Center Operations Manager 2007	Elevation of Privilege
Important	MS13-004	Microsoft Windows	Elevation of Privilege
Important	MS13-005	Microsoft Windows	Elevation of Privilege
Important	MS13-006	Microsoft Windows	Security Feature Bypass
Important	MS13-007	Microsoft Windows	Denial of Service

A summary for these new bulletins may be found at
<http://technet.microsoft.com/security/bulletin/MS13-jan>.

MICROSOFT WINDOWS MALICIOUS SOFTWARE REMOVAL TOOL

Microsoft is releasing an updated version of the Microsoft Windows Malicious Software Removal Tool on Windows Server Update Services (WSUS), Windows Update (WU) and the Download Center. Note that this tool will NOT be distributed using Software Update Services (SUS). Information on the Microsoft Windows Malicious Software Removal Tool is located here:

<http://support.microsoft.com/?kbid=890830>

HIGH-PRIORITY, NON-SECURITY UPDATES

The high priority, non-security updates that Microsoft releases, using Microsoft Update (MU), Windows Update (WU), or Windows Server Update Services (WSUS), will be detailed in the following knowledge-base article: <http://support.microsoft.com/?id=894199>

PUBLIC BULLETIN WEBCAST REPLAY

Microsoft hosts a replay of their webcast to address customer questions on these bulletins:

Title: Information about Microsoft January Security Bulletins (Level 200)

URL: <https://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032538623>

eSecurity Advisory: JANUARY 2013 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information

January 8, 2013

NEW SECURITY BULLETIN TECHNICAL DETAILS

Listed below is more technical information that may be helpful to users to protect their work and home computers. In the following tables of affected and non-affected software, software editions that are not listed are past their support lifecycle. To determine the support lifecycle for your product and edition, visit [Microsoft Support Lifecycle](#).

Customers are advised to review the information in the bulletins, and then test and deploy the updates immediately in their environments, if applicable.

Bulletin Identifier	Microsoft Security Bulletin MS13-001
Bulletin Title	Vulnerability in Windows Print Spooler Components Could Allow Remote Code Execution (2769369)
Executive Summary	This security update resolves one privately reported vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a print server received a specially crafted print job. The security update addresses the vulnerability by correcting how the Windows Print Spooler handles specially crafted print jobs.
Severity Ratings and Affected Software	This security update is rated Critical for all supported editions of Windows 7 and Windows Server 2008 R2.
Attack Vectors	A remote unauthenticated attacker could exploit the vulnerability by sending a specially crafted print job to the print server.
Mitigating Factors	Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter.
Restart Requirement	This update requires a restart.
Bulletins Replaced by This Update	None
Full Details	http://technet.microsoft.com/security/bulletin/MS13-001

eSecurity Advisory: JANUARY 2013 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information
January 8, 2013

Bulletin Identifier	Microsoft Security Bulletin MS13-002
Bulletin Title	Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (2756145)
Executive Summary	<p>This security update resolves two privately reported vulnerabilities in Microsoft XML Core Services. The vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. The security update addresses the vulnerabilities by modifying the way that Microsoft XML Core Services parses XML content.</p> <p>This security update is rated Critical for Microsoft XML Core Services 3.0, Microsoft XML Core Services 4.0, and Microsoft XML Core Services 6.0 on all affected editions of Windows XP, Windows Vista, Windows 7, Windows 8, and Windows RT.</p>
Severity Ratings and Affected Software	<p>This security update is rated Critical for Microsoft XML Core Services 5.0 when installed with all supported editions of Microsoft Office 2003, Microsoft Office 2007, Microsoft Word Viewer, Microsoft Office Compatibility Pack, Microsoft Expression Web, Microsoft SharePoint Server 2007, and Microsoft Groove Server 2007.</p> <p>This security update is rated Moderate for Microsoft XML Core Services 3.0, 4.0, and 6.0 on all affected editions of Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012.</p>
Attack Vectors	<p>A specially crafted website that is designed to invoke MSXML through Internet Explorer.</p> <p>Non-Microsoft web applications and services that utilize the MSXML library for parsing XML could also be vulnerable to this attack.</p>
Mitigating Factors	<p>In a web-based attack scenario, an attacker would have to host a website that contains a specially crafted webpage that is used to exploit this vulnerability. An attacker would have no way to force users to visit such a website. Instead, an attacker would have to convince users to visit the website, typically by getting them to click a link in an email message or Instant Messenger message that takes the user to the attacker's website.</p> <p>An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. 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.</p> <p>By default, Internet Explorer on Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 runs in a restricted mode that is known as Enhanced Security Configuration. This mode mitigates this vulnerability.</p>
Restart Requirement	This update may require a restart.
Bulletins Replaced by This Update	MS12-043
Full Details	http://technet.microsoft.com/security/bulletin/MS13-002

eSecurity Advisory: JANUARY 2013 MICROSOFT SECURITY BULLETIN RELEASEDelaware Department of Technology and Information
January 8, 2013

Bulletin Identifier	Microsoft Security Bulletin MS13-003
Bulletin Title	Vulnerabilities in System Center Operations Manager Could Allow Elevation of Privilege (2748552)
Executive Summary	This security update resolves two privately reported vulnerabilities in Microsoft System Center Operations Manager. The vulnerabilities could allow elevation of privilege if a user visits an affected website by way of a specially crafted URL. The security update addresses the vulnerabilities by modifying the way that Microsoft System Center Operations Manager accepts input.
Severity Ratings and Affected Software	This security update is rated Important for all supported editions of Microsoft System Center Operations Manager 2007.
Attack Vectors	An attacker could exploit this vulnerability by having a user visit an affected website by way of a specially crafted URL. This can be done through any medium that can contain URL web links that are controlled by the attacker, such as a link in an email, a link on a website, or a redirect on a website. In addition, compromised websites and websites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability.
Mitigating Factors	Users would have to be persuaded to open a specially crafted URL from a malicious webpage, email, or instant message.
Restart Requirement	This update does not required a restart.
Bulletins Replaced by This Update	None
Full Details	http://technet.microsoft.com/security/bulletin/MS13-003

eSecurity Advisory: JANUARY 2013 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information
January 8, 2013

Bulletin Identifier	Microsoft Security Bulletin MS13-004
Bulletin Title	Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2769324)
Executive Summary	<p>This security update resolves four privately reported vulnerabilities in the .NET Framework. The most severe of these vulnerabilities could allow elevation of privilege if a user views a specially crafted webpage using a web browser that can run XAML Browser Applications (XBAPs). The vulnerabilities could also be used by Windows .NET applications to bypass Code Access Security (CAS) restrictions. The security update addresses the vulnerabilities by correcting how the .NET Framework initializes memory arrays, copies objects in memory, validates the size of an array prior to copying objects in memory, and validates the permissions of objects.</p>
Severity Ratings and Affected Software	<p>This security update is rated Important for Microsoft .NET Framework 1.0 Service Pack 3, Microsoft .NET Framework 1.1 Service Pack 1, Microsoft .NET Framework 2.0 Service Pack 2, Microsoft .NET Framework 3.5, Microsoft .NET Framework 3.5.1, Microsoft .NET Framework 4, and Microsoft .NET Framework 4.5 on all supported editions of Microsoft Windows.</p> <p>This update has no severity rating for Microsoft .NET Framework 3.0 Service Pack 2.</p>
Attack Vectors	<p>An attacker could host a specially crafted website that contains a specially crafted XBAP (XAML browser application) that could exploit this vulnerability and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these websites. Instead, an attacker would have to convince users to visit the website, 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. It could also be possible to display specially crafted web content by using banner advertisements or by using other methods to deliver web content to affected systems.</p>
Mitigating Factors	<p>Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.</p> <p>An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. 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.</p> <p>By default, Internet Explorer 9 and Internet Explorer 10 prevent XAML, which is used by XBAPs, from running in the Internet Zone.</p> <p>By default, Internet Explorer 6, Internet Explorer 7, and Internet Explorer 8 are configured to prompt the user before running XAML, which is used by XBAPs in the Internet Zone.</p>
Restart Requirement	This update may require a restart.
Bulletins Replaced by This Update	MS10-041, MS10-077, MS12-016, MS12-025, MS12-035, MS12-038, and MS12-074.
Full Details	http://technet.microsoft.com/security/bulletin/MS13-004

eSecurity Advisory: JANUARY 2013 MICROSOFT SECURITY BULLETIN RELEASE

Delaware Department of Technology and Information
January 8, 2013

Bulletin Identifier	Microsoft Security Bulletin MS13-005
Bulletin Title	Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930)
Executive Summary	This security update resolves one privately reported vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker runs a specially crafted application. The security update addresses the vulnerability by correcting the way that the Windows kernel-mode driver handles window broadcast messages.
Severity Ratings and Affected Software	This security update is rated Important for all supported editions of Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, and Windows RT.
Attack Vectors	An attacker convinces a user to run a specially crafted application.
Mitigating Factors	An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability.
Restart Requirement	This update requires a restart.
Bulletins Replaced by This Update	MS12-078
Full Details	http://technet.microsoft.com/security/bulletin/MS13-005

Bulletin Identifier	Microsoft Security Bulletin MS13-006
Bulletin Title	Vulnerability in Microsoft Windows Could Allow Security Feature Bypass (2785220)
Executive Summary	This security update resolves a privately reported vulnerability in the implementation of SSL and TLS in Microsoft Windows. The vulnerability could allow security feature bypass if an attacker intercepts encrypted web traffic handshakes. The security update addresses the vulnerability by modifying the way that the Windows SSL provider component handles encrypted network packets.
Severity Ratings and Affected Software	This security update is rated Important for all supported editions of Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, and Windows RT.
Attack Vectors	In a man-in-the-middle attack, an attacker could inject malformed traffic into an SSL version 3 or TLS browsing session between Internet Explorer and a third-party server or a third-party client and a Microsoft server, silently downgrading the connection to SSL version 2.
Mitigating Factors	Microsoft has not identified any mitigating factors for this vulnerability.
Restart Requirement	This update requires a restart.
Bulletins Replaced by This Update	None
Full Details	http://technet.microsoft.com/security/bulletin/MS13-006

eSecurity Advisory: JANUARY 2013 MICROSOFT SECURITY BULLETIN RELEASEDelaware Department of Technology and Information
January 8, 2013

Bulletin Identifier	Microsoft Security Bulletin MS13-007
Bulletin Title	Vulnerability in Open Data Protocol Could Allow Denial of Service (2769327)
Executive Summary	This security update resolves a privately reported vulnerability in the Open Data (OData) protocol. The vulnerability could allow denial of service if an unauthenticated attacker sends specially crafted HTTP requests to an affected site. The security update addresses the vulnerability by turning off the WCF Replace function by default.
Severity Ratings and Affected Software	This security update is rated Important for Microsoft .NET Framework 3.5, Microsoft .NET Framework 3.5 Service Pack 1, Microsoft .NET Framework 3.5.1, and Microsoft .NET Framework 4. It is also rated Important for Management OData IIS Extension when installed on Microsoft Windows Server 2012.
Attack Vectors	An unauthenticated attacker could send a small number of specially crafted HTTP requests to an affected site, causing a denial of service condition.
Mitigating Factors	Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.
Restart Requirement	This update may require a restart.
Bulletins Replaced by This Update	None
Full Details	http://technet.microsoft.com/security/bulletin/MS13-007

PLEASE VISIT [HTTP://WWW.MICROSOFT.COM/TECHNET/SECURITY](http://www.microsoft.com/technet/security)
FOR THE MOST CURRENT INFORMATION ON THESE ALERTS