



## eSecurity Advisory AUGUST 2012 MICROSOFT SECURITY BULLETIN RELEASE

The purpose of this update is to provide you with a summary of the Microsoft August 2012 Security Bulletin release.

### NEW BULLETINS

Microsoft released the following security bulletins for newly discovered vulnerabilities:

Severity	Bulletin ID	Affected Product	Impact
Critical	MS12-052	Microsoft Internet Explorer	Remote Code Execution
Critical	MS12-053	Microsoft Windows	Remote Code Execution
Critical	MS12-054	Microsoft Windows	Elevation of Privilege
Important	MS12-055	Microsoft Windows	Remote Code Execution
Important	MS12-056	Microsoft Windows	Remote Code Execution
Important	MS12-057	Microsoft Office	Remote Code Execution
Critical	MS12-058	Microsoft Exchange Server	Remote Code Execution
Important	MS12-059	Microsoft Office	Remote Code Execution
Critical	MS12-060	Microsoft Commerce Server, Microsoft Office, Microsoft SQL Server	Remote Code Execution

A summary for these new bulletins may be found at  
<http://technet.microsoft.com/security/bulletin/MS12-Aug>.

---

### 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 will host a webcast to address customer questions on these bulletins:

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

URL: <https://msevents.microsoft.com/CUI/EventDetail.aspx?EventID=1032522555&Culture=en-US>

**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.**

**Cumulative Security Update for Internet Explorer (2722913)**

**Microsoft Security Bulletin MS12-052**

**Summary:** This security update resolves four privately reported vulnerabilities in Internet Explorer. The most severe 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 Internet Explorer handles objects in memory.

**Severity:** **Critical**

**Affected:** Microsoft Internet Explorer  
*For more information, see the subsection, "Affected and Non-Affected Software" at the link below.*

**Impact:** Remote Code Execution

**Details:** <http://technet.microsoft.com/en-us/security/bulletin/ms12-052>

[Back to Top](#)

**Vulnerability in Remote Desktop Could Allow Remote Code Execution (2723135)**

**Microsoft Security Bulletin MS12-053**

**Summary:** This security update resolves a privately reported vulnerability in the Remote Desktop Protocol. The vulnerability could allow remote code execution if an attacker sends a sequence of specially crafted RDP packets to an affected system. The security update addresses the vulnerability by modifying the way that the Remote Desktop Protocol processes packets in memory.

**Severity:** **Critical**

**Affected:** Microsoft Windows  
*For more information, see the subsection, "Affected and Non-Affected Software" at the link below.*

**Impact:** Remote Code Execution

**Details:** <http://technet.microsoft.com/en-us/security/bulletin/ms12-053>

[Back to Top](#)

## **Vulnerabilities in Windows Networking Components Could Allow Remote Code Execution (2733594)**

### **Microsoft Security Bulletin MS12-054**

**Summary:** This security update resolves four privately reported vulnerabilities in Microsoft Windows. The most severe of these vulnerabilities could allow remote code execution if an attacker sends a specially crafted response to a Windows print spooler request. The security update addresses the vulnerabilities by correcting how the Windows Print Spooler handles specially crafted responses and how Windows networking components handle Remote Administration Protocol (RAP) responses.

**Severity:** **Critical**

**Affected:** Microsoft Windows  
*For more information, see the subsection, "Affected and Non-Affected Software" at the link below.*

**Impact:** Remote Code Execution

**Details:** <http://technet.microsoft.com/en-us/security/bulletin/ms12-054>

[Back to Top](#)

## **Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2731847)**

### **Microsoft Security Bulletin MS12-055**

**Summary:** This security update resolves one privately reported vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. The security update addresses the vulnerabilities by correcting the way that the Windows kernel-mode driver handles objects in memory.

**Severity:** **Important**

**Affected:** Microsoft Windows  
*For more information, see the subsection, "Affected and Non-Affected Software" at the link below.*

**Impact:** Elevation of Privilege

**Details:** <http://technet.microsoft.com/en-us/security/bulletin/ms12-055>

[Back to Top](#)

## **Vulnerability in JScript and VBScript Engines Could Allow Remote Code Execution (2706045)**

### **Microsoft Security Bulletin MS12-056**

**Summary:** This security update resolves a privately reported vulnerability in the JScript and VBScript scripting engines on 64-bit versions of Microsoft Windows. The vulnerability could allow remote code execution if a user visited a specially crafted website. The security update addresses the vulnerability by modifying the way that JScript and VBScript handle objects in memory.

**Severity:** **Important**

**Affected:** Microsoft Windows  
*For more information, see the subsection, "Affected and Non-Affected Software" at the link below.*

**Impact:** Elevation of Privilege

**Details:** <http://technet.microsoft.com/en-us/security/bulletin/ms12-056>

[Back to Top](#)

## **Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)**

### **Microsoft Security Bulletin MS12-057**

**Summary:** This security update resolves one privately reported vulnerability in Microsoft Office. The vulnerability could allow remote code execution if a user opens a specially crafted file or embeds a specially crafted Computer Graphics Metafile (CGM) graphics file into an Office file. The security update addresses the vulnerability by disabling the loading of CGM graphics files in Microsoft Office applications.

**Severity:** **Important**

**Affected:** Microsoft Office  
*For more information, see the subsection, "Affected and Non-Affected Software" at the link below.*

**Impact:** Remote Code Execution

**Details:** <http://technet.microsoft.com/en-us/security/bulletin/ms12-057>

[Back to Top](#)

## **Vulnerabilities in Microsoft Exchange Server WebReady Document Viewing Could Allow Remote Code Execution (2740358)**

### **Microsoft Security Bulletin MS12-058**

**Summary:** This security update resolves publicly disclosed vulnerabilities in Microsoft Exchange Server WebReady Document Viewing. The vulnerabilities could allow remote code execution in the security context of the transcoding service on the Exchange server if a user previews a specially crafted file using Outlook Web App (OWA). The security update addresses the vulnerabilities by updating the affected Oracle Outside In libraries to a non-vulnerable version.

**Severity:** **Critical**

**Affected:** Microsoft Exchange Server  
*For more information, see the subsection, "Affected and Non-Affected Software" at the link below.*

**Impact:** Remote Code Execution

**Details:** <http://technet.microsoft.com/en-us/security/bulletin/ms12-058>

[Back to Top](#)

## **Vulnerability in Microsoft Visio Could Allow Remote Code Execution (2733918)**

### **Microsoft Security Bulletin MS12-059**

**Summary:** This security update resolves a privately reported vulnerability in Microsoft Office. The vulnerability could allow remote code execution if a user opens a specially crafted Visio file. The security update addresses the vulnerabilities by correcting the way that Microsoft Office Visio validates data when parsing specially crafted Visio files.

**Severity:** **Important**

**Affected:** Microsoft Office  
*For more information, see the subsection, "Affected and Non-Affected Software" at the link below.*

**Impact:** Remote Code Execution

**Details:** <http://technet.microsoft.com/en-us/security/bulletin/ms12-059>

[Back to Top](#)

## **Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2720573)**

### **Microsoft Security Bulletin MS12-060**

**Summary:** This security update resolves a privately reported vulnerability in Windows common controls. The vulnerability could allow remote code execution if a user visits a website containing specially crafted content designed to exploit the vulnerability. The malicious file could be sent as an email attachment as well, but the attacker would have to convince the user to open the attachment in order to exploit the vulnerability. The security update addresses the vulnerability by disabling the vulnerable version of the Windows common controls and replacing it with a new version that does not contain the vulnerability.

**Severity:** **Critical**

**Affected:** Microsoft Office  
*For more information, see the subsection, "Affected and Non-Affected Software" at the link below.*

**Impact:** Remote Code Execution

**Details:** <http://technet.microsoft.com/en-us/security/bulletin/ms12-060>

[Back to Top](#)

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