

11 February 2009

By: Marius Oiaga, Technology News Editor

Internet Explorer  
Microsoft

## [IE8 in Windows 7, and IE7 in Vista SP2 - Download Critical Patches](#)

[Available right here](#)

Concomitantly with the availability of the IE Cumulative Security Update for February 2009 via Windows Update, Microsoft also released security patches for pre-release and final versions of Internet Explorer running on operating systems still in development or already RTM'd. The security updates are designed to resolve a couple of Critical vulnerabilities in Internet Explorer 8 Beta 2 for Windows Vista SP1, Windows XP SP3, Windows Server 2003, and Windows Server 2008, for the IE8 Beta build in [Windows 7](#) pre-Beta and in Windows Server 2008 R2 pre-Beta, but also for Internet Explorer 7 running on top of [Windows Vista Service Pack 2 \(Beta\)](#) and Windows Server 2008 SP2 Beta.

"Uninitialized Memory Corruption Vulnerability - CVE-2009-0075 - a remote code execution vulnerability exists in the way Internet Explorer accesses an object that has been deleted. An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user," Microsoft revealed.

At the end of January 2009, Microsoft made available for download the first and only [Release Candidate for Internet Explorer 8](#). At the same time, Windows 7 Beta started being offered as a public download on January 10, 2009, along with Windows Server 2008 R2 Beta. [Windows Vista Service Pack 2 Beta and Windows Server 2008 SP2 Beta](#) are up for grabs since December 2008.

"CSS Memory Corruption Vulnerability - CVE-2009-0076 - a remote code execution vulnerability exists in the way Internet Explorer handles Cascading Style Sheets (CSS). An attacker could exploit the vulnerability by constructing a specially crafted Web page. When a user views the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user," Microsoft added.

Here are the links to the security updates:

- [Security Update for Internet Explorer 8 Beta 2 for Windows XP \(KB961260\)](#)
- [Security Update for Internet Explorer 8 Beta 2 for Windows XP x64 Edition \(KB961260\)](#)
- [Security Update for Internet Explorer 8 Beta 2 for Windows Server 2003 \(KB961260\)](#)
- [Security Update for Internet Explorer 8 Beta 2 for Windows Server 2003 x64 Edition \(KB961260\)](#)
- [Security Update for Internet Explorer 8 Beta 2 in Windows Vista \(KB961260\)](#)
- [Security Update for Internet Explorer 8 Beta 2 in Windows Vista x64 Edition \(KB961260\)](#)
- [Security Update for Internet Explorer 8 Beta 2 in Windows Server 2008 \(KB961260\)](#)
- [Security Update for Internet Explorer 8 Beta 2 for Windows Server 2008 x64 Edition \(KB961260\)](#)
- [Security Update for Internet Explorer 8 in Windows 7 Client Pre-Beta \(KB961260\)](#)
- [Security Update for Internet Explorer 8 in Windows 7 Server Pre-Beta 64-bit Itanium Edition \(KB961260\)](#)
- [Security Update for Internet Explorer 8 in Windows 7 Client Pre-Beta for x64-based Systems \(KB961260\)](#)

- [Security Update for Internet Explorer 8 in Windows 7 Server Pre-Beta for x64-based Systems \(KB961260\)](#)
- [Security Update for Internet Explorer in Windows Server 2008 64-bit Itanium Edition \(KB961260\)](#)
- [Security Update for Internet Explorer 7 in Windows Server 2008 Service Pack 2 \(KB961260\)](#)
- [Security Update for Internet Explorer 7 in Windows Server 2008 Service Pack 2 x64 Edition \(KB961260\)](#)
- [Security Update for Internet Explorer 7 in Windows Vista Service Pack 2 \(KB961260\)](#)
- [Security Update for Internet Explorer 7 in Windows Vista Service Pack 2 x64 Edition \(KB961260\)](#)