

8 May 2008

By: Marius Oiaga, Technology News Editor

Windows Update  
Microsoft

## [Critical Security Patch for Windows XP Service Pack 3 Final](#)

*Released concomitantly with SP3*

**Windows XP SP3** was barely out the door, when Microsoft rushed to issue the first critical patch for the service pack. Concomitantly with the general availability of the last service pack for XP, Microsoft dropped the first critical security update designed to patch Internet Explorer 7 running on XP SP3 RTM Build 5512. [IE7-WindowsXP-KB947864-x86-ENU.exe](#) is designed for both XP SP2 and XP SP3, and was initially offered on May 6, 2008, after downloads containing the latest service pack for XP went live via Windows Update and the Download Center. "This update addresses the vulnerability discussed in Microsoft Security Bulletin MS08-024," Microsoft informed. "Security issues have been identified that could allow an attacker to compromise a computer running Microsoft Internet Explorer and gain control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer." Microsoft Security Bulletin MS08-024 labeled with a maximum severity rating of Critical was released on April 8, 2008, and then updated after the RTM of XP SP3 on April 22 and 23. Microsoft "added Internet Explorer 7 for Windows XP Service Pack 3 to affected software. [And then] removed erroneous references to Windows XP Professional x64 Edition Service Pack 3," the company informed. The original security bulletin MS08-024 was designed to patch a critical security flaw in IE5, IE6 and IE7. IE7-WindowsXP-KB947864-x86-ENU.exe however is limited only to IE7 on XP SP3, as Internet Explorer 6 which ships with the service pack as a default component already features the patch. "A remote code execution vulnerability exists in Internet Explorer because of the way that it processes data streams. 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.