

15 October 2007

By: Marius Oiaga, Technology News Editor

Security
Microsoft

[Internet Explorer 7 Is an Open Door for Attacks](#)

On Windows XP and Windows Server 2003

Internet Explorer 7 on Windows XP and Windows Server 2003 is nothing short of an open door for attacks. Microsoft informed that it is currently investigating a remote code execution vulnerability in various versions of XP and Windows Server 2003 running Internet Explorer 7. The Redmond company added that Windows Vista users are safe, although the operating system comes with IE7 built in by default. Windows XP SP2, XP Professional x64 Edition, Professional x64 Edition SP2; Windows Server 2003 SP1 and SP2, Windows Server 2003 x64 Edition and SP2 and Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems are all vulnerable to the security flaw, provided they are running IE7. The vulnerability is related to the way the Windows operating system handles Uniform Resource Identifiers (URIs). "When a user clicks a link to a URI, the application showing that link to users decides how it is supposed to be handled. For traditionally "safe" protocols like mailto: or http: applications often just verify the prefix and then choose to call into the Windows shell32 function ShellExecute() to handle it. This has been the case for a number of years. Windows then launches Internet Explorer passing the URI or launches the preferred email client passing the email address etc. With IE6 installed, ShellExecute() passes the URI to IE which accepts it and inside IE determines it to be invalid. Navigation then fails harmlessly. With Internet Explorer 7 installed, the flow is a bit different", explained Jonathan Ness with the SWI team at Microsoft Security Response Center. With IE7, Microsoft has implemented additional validation in the process of rejecting a malformed URI. Essentially, malformed URIs will no longer be rejected up front, and instead would be moved to ShellExecute() in order to be fixed. When ShellExecute() is handling URIs in order to make them usable, the process is not safely managed. In Vista, for example, ShellExecute() also rejects the URI, but the copies of Windows XP and Windows Server 2003 do not deliver a similar behavior. Microsoft emphasized that the vulnerability can be successfully exploited only in the limited contexts described above, and that other versions of the Windows operating system with IE7 installed are not affected. "Our plan is to revise our URI handling code within ShellExecute() to be more strict. While our update will help protect all applications from malformed URI's, application vendors who handle URI's can also do stricter validation themselves to prevent malicious URI's from being passed to ShellExecute(). We have seen several vendors introduce additional validation as a way to protect their customers from this issue", Ness added.