

18 April 2008

By: Marius Oiaga, Technology News Editor

[Vista SP1 RTM Hit by New Hole, XP SP3 Safe](#)

The new vulnerability allows elevation of privilege



[Windows XP Service Pack 3](#), despite the fact that it is yet to be released in its final version, is safe from the latest security vulnerability impacting a range of Windows platforms including XP SP2 and [Vista SP1](#). Despite the fact that Windows Vista was constantly applauded throughout 2007 as the safest version of Windows available on the market, the operating system is in no way bulletproofed. And even with Service Pack 1, an update designed to increase security, among other things, Vista is still susceptible to attacks exploiting security holes. Of course that Microsoft has failed to reveal why XP SP3 is not on the list with the affected operating systems. In this regard, the company could have already patched XP SP3, or is simply ignoring the final service pack for Windows XP until its finalization. [Bill Sisk](#), Microsoft Security Response Center Communications Manager, informed of "a new public report of a vulnerability within Microsoft Windows which allows for privilege escalation from authenticated user to LocalSystem. Our investigation has shown that this vulnerability affects Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008." Both the 32-bit and 64-bit versions of Vista SP1 RTM are affected. According to the Redmond company, in the eventuality of a successful exploit, an attacker could use the flaw in order to perform an "elevation of privilege from authenticated user to LocalSystem." Microsoft warned of a few scenarios where customers would be at increased risk. Hosting providers and organizations permitting the execution of user-provided code in authenticated contexts (using Internet Information Services (IIS) and SQL Server) should work to mitigate the threat until a patch will be in place. Microsoft recommends the following mitigations for customers running IIS 6.0 (Configure a Worker Process Identity (WPI) for an application pool in IIS to use a created account in IIS Manager and disable MSDTC); IIS 7.0 - Specify a WPI for an application pool in IIS Manager or Specify a WPI for an application pool using the Command Line utility APPCMD.exe. The mitigations are available [here](#). "At this time, we are not aware of attacks attempting to use the reported vulnerability, but we will continue to track this issue. The advisory contains several workarounds that customers can use to help protect themselves. Upon completion of this investigation, Microsoft will take the appropriate action to help protect our customers. This may include providing a security update through our monthly release," Sisk added.