

5 January 2009

By: Marius Oiaga, Technology News Editor

[New Malware Targets Windows 7, Vista SP1 and XP SP3 Vulnerability](#)

Worm:Win32/Conficker.B

Windows
Microsoft

Worm:Win32/Conficker.B is a new piece of malware targeting a [vulnerability in Server Service](#) affecting all supporter versions of Windows, including Windows 7, Windows Vista SP1, and Windows XP SP3. Microsoft published details related to the new malicious code designed to exploit the MS08-067 Critical vulnerability reported in 2008, and patched with an out-of-band security update in October. Essentially, the software giant informed that Worm:Win32/Conficker.B was a variant of the Worm:Win32/Conficker malware, which was initially associated with attacks against [MS08-067](#).

"We've seen another resurgence of Worm:Win32/Conficker, this time as Worm:Win32/Conficker.B. We've already received a number of reports of this new variant from the wild from affected users. Not surprisingly, a majority of the new infections we're seeing are on machines that are yet to install the MS08-067 update. This new variant also spreads via network shares by attempting to log in to machines using a list of weak, common, and predictable passwords. Make sure you install those patches guys and keep your anti-Virus solution up to date," [Matt McCormack](#), MMPC Melbourne, revealed.

By exploiting the Windows Server service (SVCHOST.EXE) vulnerability, the worm is capable of infecting computers across a network. The Redmond company pointed out that successful exploit could lead to remote code execution in scenarios in which file sharing was enabled on vulnerable machines. Win32/Conficker is also known as TA08-297A, CVE-2008-4250, VU827267, Win32/Conficker.A (CA), Mal/Conficker-A (Sophos), Trojan.Win32.Agent.bccs (Kaspersky), and W32.Downadup.B (Symantec).

In order to bulletproof themselves against exploits targeting the SVCHOST.EXE vulnerability, Windows users are advised to deploy MS08-067 immediately. The security bulletin has now been available for a couple of months on Windows Update, and Windows operating systems with Automatic Updates enabled have already deployed the patch. Microsoft informed that while both Windows client and server operating systems were affected because of the mitigations introduced in Vista Windows Server 2008 and Windows 7, the vulnerability on these platforms was rated only Important and not Critical.

"This vulnerability was reported after the release of Windows 7 Pre-Beta. Customers running Windows 7 Pre-Beta are encouraged to download and apply the update to their systems. On Windows 7 Pre-Beta systems, the vulnerable code path is only accessible to authenticated users. This vulnerability is not liable to be triggered if the attacker is not authenticated, and therefore would be rated Important," Microsoft explained.