

6 November 2008

By: Marius Oiaga, Technology News Editor

Security
Microsoft

[Vista SP1 and XP SP3 Vulnerability Hit by Malware](#)

Even though it is already patched

Microsoft issued a warning related to the detection of new examples of malicious code in attacks attempting to exploit a vulnerability affecting various Windows client and server releases. In October, the Redmond giant put out an out-of-band security patch designed to plug a vulnerability residing in the Server Service on Windows systems. According to the company, a successful exploit of the security flaw would lead to remote code execution. The patch was released on October 23, 2008, and will render attacks useless.

"We have seen some new pieces of malware attempting to exploit this vulnerability this week. And while so far, none of these attacks are the broad, fast-moving, self-replicating attacks people usually think of when they hear the word 'worm,' they do underscore the importance of deploying this update if you haven't already," revealed Security Response Communications Lead, [Christopher Budd](#).

Budd indicated that Microsoft was seeing consistent deployments of the MS08-067 patch, and urged customers that had failed to update so far to do so as soon as possible. At the same time, Microsoft provided a list of malware built to exploit the Server Service vulnerability, including: Trojan:Win32/Wecorl.A; Trojan:Win32/Wecorl.B; Trojan:Win32/Clort.A; Trojan:Win32/Clort.A!exploit; Trojan:Win32/Clort.A.dr; TrojanDownloader:Win32/VB.CQ and TrojanDownloader:Win32/VB.CJ.

"None of these are broad, fast-moving, self-replicating attacks. They're similar to the original attacks we detected, in that they focus on loading malware onto vulnerable system. They're also similar in that the overall scope of these attacks is very limited. The largest of these attacks are those associated with Clort family and we've seen well below fifty attacks worldwide," Budd said, adding that Microsoft was only aware of limited attacks attempting to exploit the vulnerability, and not of a widespread threat.