

TopResponse Threat Advisory

Release Date: April 15, 2010

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against the Microsoft SMB Client Message Size Vulnerability (MS10-020, CVE-2010-0477).

Top Layer Products: IPS 5500 v4.X and higher.

Vulnerable Infrastructure: Microsoft Windows 7 for 32-bit and x64-based Systems, Microsoft Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems SP2, Microsoft Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems SP2, and Windows Server 2008 R2 for x64-based Systems.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems

Advisory Impact: Prevention

Summary: Microsoft Windows Server Message Block (SMB) is a file sharing protocol used by default. Version 2.0 of SMB is only supported on Microsoft Windows Vista, Windows Server 2008 and Windows 7. The vulnerability can be exploited by a malicious SMB server or man-in-the-middle attack. By enticing the victim to mount files from the malicious SMB server, the attacker can send a specially crafted SMB response to execute arbitrary code on the system. The IPS 5500 provides proactive protection for this vulnerability.

Recommended Action: Top Layer recommends the following actions:

Ensure that the rule tln-005031, "PROTO: CIFS Protocol Error", is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft systems that have the SMBv2 service enabled. The rule is currently enabled in the "Recommended Client Protection" and "Recommended Server Protection" IPS Rule Sets.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/Bulletin/MS10-020.msp
Mitre CVE Advisory	http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0477

Relevant TLN Rules: tln-005031