

TopResponse Threat Advisory

Release Date: September 9, 2009

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against the Microsoft SMB v2 Array Index Denial of Service Vulnerability (CVE-2009-3103).

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

Vulnerable Infrastructure: Microsoft Windows Vista, Windows Vista SP1 and SP2, Windows Vista x64 Edition, Windows Vista x64 Edition SP1 and SP2, Microsoft Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems SP2, Microsoft Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems SP2, and Microsoft Windows Server 2008 for Itanium-based Systems, as well as Windows Server 2008 for Itanium-based Systems SP2.

Alert Type: Denial of Service

Risk Assessment: High

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to crash the system repeatedly.

Advisory Impact: Prevention

Summary: Microsoft Windows SMB v2 protocol is used by Microsoft infrastructure to share system resources such as files and printers. The vulnerability involves an invalid character sent in the NEGOTIATE PROTOCOL REQUEST packet. The resulting memory corruption could allow an attacker to repeatedly crash the vulnerable system with a single unauthenticated network packet. The IPS 5500 provides proactive protection for this vulnerability.

Recommended Action: Top Layer recommends the following actions:

Ensure that the rule tln-005022, "PROTO: CIFS Protocol Field Error", is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft systems that have SMB v2 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/advisory/975497.mspx
Mitre CVE Advisory	http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103

Relevant TLN Rules: tln-005022