

TopResponse Threat Advisory

Release Date: January 11, 2011

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Microsoft Windows Backup Manager DLL Hijacking Remote Code Execution (MS11-001,CVE-2010-3145) Vulnerability.

Top Layer Products: IPS 5500 and higher.

Vulnerable Infrastructure: Microsoft Windows Vista SP1, Microsoft Windows Vista SP2, Microsoft Windows Vista x64 Edition SP1 and SP2.

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: The Microsoft Windows Backup Manager allows users to restore system files to an earlier point in time. The reported vulnerability could allow a remote attacker to execute arbitrary code on the systems running the Microsoft Backup Manager software by enticing a user to visit a specially crafted web site that causes vulnerable systems to attempt to download a file using either the WebDAV or the Microsoft RPC protocol. The IPS 5500 provides proactive protection against known attacks targeting this vulnerability.

Recommended Action: Top Layer recommends the following actions:

Ensure that the rule tln-102004, “AAUPV: HTTP Method Name Matches Specified Filter”, is enabled in the IPS Rule Set that is used to inspect traffic sent from your Microsoft Windows Backup Manager infrastructure. The rule is currently enabled in the “Strict Server Protection” IPS Rule Set.

Note: IPS rule tln-102004 is currently enabled in the Strict IPS Rule Set because there is a potential for false positive events. Please monitor events after the rules are enabled to provide protection for this vulnerability.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/Bulletin/MS11-001.msp

Relevant TLN Rules: tln-102004.