

TopResponse Threat Advisory

Release Date: January 7, 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 Address Book DLL Hijacking Remote Code Execution (MS10-096,CVE-2010-3147) and Microsoft Windows Connection Signup Wizard DLL Hijacking Remote Code Execution (MS10-097,CVE-2010-3144) Vulnerabilities.

Top Layer Products: IPS 5500 and higher.

Vulnerable Infrastructure: Microsoft Windows XP SP3, Microsoft Windows Server 2003 SP2, Microsoft Windows 7 for 32-bit Systems, Microsoft Windows Server 2008 R2 for x64-based Systems, and other software versions as specified in the Microsoft advisories for the vulnerabilities.

Alert Type: Critical vulnerabilities

Risk Assessment: Critical

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

Advisory Impact: Prevention

Summary: The Microsoft Windows Address Book and Microsoft Windows Connection Signup Wizard software are vulnerable to DLL Hijacking. The reported vulnerabilities could allow a remote attacker to execute arbitrary code on the systems running the Microsoft Windows Address Book and Microsoft Windows Connection Signup Wizard software by enticing a user on the systems to visit a specially crafted web site that causes vulnerable systems to attempt to download a file from an external system using either the WebDAV or the Microsoft RPC protocol. The IPS 5500 provides proactive protection against known attacks targeting these vulnerabilities.

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 Address Book and Microsoft Windows Connection Signup Wizard 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/MS10-096.msp |
| Microsoft Advisory | http://www.microsoft.com/technet/security/Bulletin/MS10-097.msp |

Relevant TLN Rules: tln-102004.