

TopResponse Threat Advisory

Release Date: April 15, 2009

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection for the Microsoft Windows HTTP Services Vulnerability (MS09-013, CVE-2009-0086).

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

Vulnerable Infrastructure: Microsoft Windows 2000 SP4, Windows XP SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 x64 Edition SP2, Windows Vista SP1, Windows Vista x64 Edition SP1, Windows Server 2008.

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 Windows HTTP Services (WinHTTP) provides a HTTP client application programming interface (API) that enables applications to send HTTP requests to remote Web servers. WinHTTP is found in both vendor applications and Microsoft Windows components, such as the Universal Plug and Play (UPNP) and Windows Media Player. The vulnerability could allow an attacker to execute arbitrary code on the client system with the same privileges as the application or service that utilized the WinHTTP API.

Recommended Action: Top Layer recommends the following actions:

Ensure that the rule tln-102063, "AAUPV: HTTP Chunked Encoding Length Too Long", is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft systems. 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 Web site	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/bulletin/MS09-013.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0086

Relevant TLN Rules: tln-102063