

TopResponse Threat Advisory

Release Date: March 11, 2009

Updated: March 23, 2009

Purpose: The Top Layer TopResponse team is issuing an advisory which provides information needed to provide protection for the Microsoft DNS and WINS Services WPAD Spoofing Vulnerabilities (MS09-008, CVE-2009-0093, CVE-2009-0094).

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

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

Alert Type: Spoofing Vulnerability

Risk Assessment: High

Threat Impact: DNS and WINS poisoning for Windows Proxy Auto Discovery (WPAD) configuration.

Advisory Impact: Prevention

Summary: Microsoft DNS and WINS Services provide client infrastructure with name resolution. The vulnerability could allow a remote attacker to register the values for the Windows Proxy Auto Discovery (WPAD) in the DNS or WINS server. The WPAD information is requested by web browsers configured to automatically detect proxy configurations on the local network. Once the DNS or WINS server is under the attacker's control, WPAD requests would point dependent client browsers to a malicious web proxy.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2009-03-10-03 (or later) to put this new protection into place. This Protection Pack provides additional layers of detection and defense for a vulnerability that is publicly disclosed, via the new rules tln-106233 and tln-103049. Please review what rules are valid for your deployment.

For IPS 5500 v4.X and higher customers: Ensure that the rule tln-106233, “AAUPV: Microsoft DNS Server WPAD Registration”, is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft DNS or WINS servers. The rule is currently enabled to block in the “Strict Client Protection” and “Strict Server Protection” IPS Rule Sets. In addition, the rule tln-106233 is set to detect the WPAD registration as part of the "Recommended Client Protection - Detect Only" and the "Recommended Server Protection - Detect Only" IPS Rule Sets.

For IPS 5500 E-Series customers: Also ensure that the rule tln-103049, “AAUPV: HTTP URI Prefix Matches Filter: Wpad Access”, is enabled in the IPS Rule Set that is used to inspect traffic sent by your Microsoft client infrastructure. The protection is enforced on the client request for the WPAD configuration data. The rule is currently enabled in the “Strict Client Protection” and “Strict 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/MS09-008.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0093 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0094

Relevant TLN Rules: tln-103049 and tln-106233