

TopResponse Threat Advisory

Release Date: August 12, 2009

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Windows Workstation Service Memory Corruption Vulnerability (MS09-041, CVE-2009-1544).

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

Vulnerable Infrastructure: Windows XP SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 x64 Edition SP2, Windows Server 2003 with SP2 for Itanium-based Systems, Windows Vista SP2, Windows Vista x64 Edition SP2, Windows Server 2008 for 32-bit Systems SP2, Windows Server 2008 for x64-based Systems SP2, and Windows Server 2008 for Itanium-based Systems SP2.

Alert Type: Moderate Vulnerability

Risk Assessment: Important

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

Advisory Impact: Prevention

Summary: Microsoft Windows Workstation Service is the system component responsible for routing remote RPC requests for local file and printer resources. The reported vulnerability could allow an attacker to load arbitrary code into the running Windows Workstation Service process by exploiting an issue in the management of previously released memory allocations. The vulnerability is delivered to the target system by sending a specially crafted RPC request.

Recommended Action: Top Layer recommends the following actions:

Ensure that the IPS rule tln-008005, “PROTO: MSRPC Invalid Stub Data Length”, is enabled in the IPS Rule Set used to inspect traffic to your Microsoft hosts. This rule is currently enabled in the “Recommended Client Protection” and “Recommended Server Protection” IPS Rule Sets.

Download and apply Protection Pack 2009-08-12-01 (or later) to provide protection against this vulnerability. IPS rule tln-008005 has been enhanced for the Microsoft Windows Workstation Service Memory Corruption Vulnerability (MS09-041, CVE-2009-1544).

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/bulletin/MS09-041.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1544

Relevant TLN Rules: tln-008005

Relevant TopResponse Protection Pack(s): 2009-08-12-01