

TopResponse Threat Advisory

Release Date: June 09, 2009

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Windows Print Spooler Load Library Vulnerability (MS09-022, CVE-2009-0230).

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 SP2, Windows Vista x64 Edition SP2, Windows Server 2008 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 Print Spooler Service is the system component responsible for responding to remote RPC requests to local hosted printers. The service allows authenticated and anonymous connections. The reported vulnerability could allow an authenticated attacker to load an arbitrary library that currently exists on the user's system into the running Windows Print Spooler Service process 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 2009-06-09-02 (or later) to provide protection against this vulnerability. IPS rule tln-008005 has been enhanced for the Microsoft Windows Print Spooler Load Library Vulnerability (MS09-022, CVE-2009-0230) .

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/MS09-022.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1532

Relevant TLN Rules: tln-008005

Relevant TopResponse Protection Pack(s): 2009-06-09-02