

## TopResponse Threat Advisory

**Release Date:** October 23, 2008

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Server Service RPC Vulnerability (MS08-067,CVE-2008-4250).

**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:** Microsoft Server Service is the system component responsible for responding to remote RPC requests to local resources such as file sharing and local hosted printers. The service allows authenticated and anonymous connections. The reported vulnerability could allow an attacker to execute arbitrary code on the user's 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 2008-10-23-03 (or later) to provide protection against post-exploitation attempts by known exploits of the reported vulnerability. The SANS\_DSshield blocked IP address list has been updated to incorporate known malicious sites. Ensure that your IPS Unit's Security Policy table contains a policy row configured to block traffic to or from the SANS\_DSshield Host Group.

**References:** Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
Microsoft Advisory	<a href="http://www.microsoft.com/technet/security/bulletin/MS08-067.msp">http://www.microsoft.com/technet/security/bulletin/MS08-067.msp</a>

**Relevant TLN Rules:** tln-008005

**Relevant TopResponse Protection Pack(s):** 2008-10-23-03