

## TopResponse Threat Advisory

**Release Date:** January 10, 2008

**Purpose:** The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against the critical Microsoft Windows Kernel ICMP Router Advertisement Vulnerability (CVE-2007-0066).

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

**Vulnerable Infrastructure:** Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Server 2003.

**Alert Type:** Recommendations regarding a recent vulnerability

**Risk Assessment:** Critical

**Threat Impact:** Denial of service

**Advisory Impact:** Prevention

**Summary:** The Microsoft Windows kernel contains a driver that supports processing of the ICMP queries. The processing performed by the driver includes parsing of the Router Discovery Protocol (RDP) messages over ICMP, such as an RDP Router Advertisement message embedded in an ICMP query. The reported vulnerability could allow an attacker to cause a denial of service on a user system by sending a specially crafted ICMP query containing an RDP Router Advertisement.

**Recommended Action:** Top Layer recommends the following actions:

Ensure that the rule tln-003003, "PROTO: ICMP Frame Length Illegal For Type Or Exceeds Specified Limit," is enabled in the policies that provide protection for the infrastructure running vulnerable Microsoft products.

**Note:** This rule is enabled by default in the "Recommended Client Protection" and "Recommended Server Protection" IPS Rule Sets.

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

| <b>Additional Information</b>     | <b>Location</b>   |
|-----------------------------------|---|
| <b>Top Layer Support Web site</b> | <a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>   |
| <b>Microsoft Advisory</b>         | <a href="http://www.microsoft.com/technet/security/Bulletin/MS08-001.msp">http://www.microsoft.com/technet/security/Bulletin/MS08-001.msp</a> |

**Relevant TLN Rules:** TLN-003003