

TopResponse Threat Advisory

Release Date: August 9, 2006

Purpose: The Top Layer TopResponse team reminds customers that existing IPS security features provide proactive protection against critical vulnerabilities released by Microsoft on August 8, 2006.

Top Layer Products: IPS 5500 Version 3.40 and higher and AM-IPS 3500 version 2.10 and above.

Vulnerable Infrastructure: Microsoft Windows 2000 Service Pack 4, Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2, Microsoft Windows XP Professional x64 Edition, Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1, Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems, Microsoft Windows Server 2003 x64 Edition.

Alert Type: Recommendations regarding a recent Microsoft vulnerability

Risk Assessment: Critical

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

Advisory Impact: Prevention

Summary: Several critical and important vulnerabilities have recently been reported by Microsoft. The IPS5500 provides proactive protection against the Microsoft Windows DNS Client Buffer Overrun Vulnerability (CVE-2006-3441). The IPS5500 also provides proactive protection against the Microsoft Server Service Buffer Overrun Vulnerability (CVE-2006-3439) through the Top Layer recommended firewall protection as further described in the Top Layer Cumulative Filter Advisory issued in August of 2005.

Recommended Action: For the IPS 5500 Version 3.40 and higher, Top Layer recommends the following actions:

1. Install patches for the vulnerable software as recommended by Microsoft.
2. Ensure that the rule tln-101052, "DNS Inbound Resource Record Type Matches Specified Filter", is enabled in the policies that provide protection for your DNS infrastructure.

Note: This rule is enabled by default in the recommended client and server protection sets.

3. Use the firewall section in the IPS5500 to block all unsolicited incoming traffic from the Internet for the following services:

Service Name	Service	Firewall Action
nbiosSn/tcp139	139	Drop
nbiosSn/udp139	139	Drop
msds/tcp445	445	Drop
msds/udp445	445	Drop

Note: It is essential that you correctly identify legitimate services that are using the ports described above before implementing a block rule or the services could be impacted inadvertently. If a Service does not exist, use Configure Security → Services → Add Service to create it. Then, add the Service to a list of services to be blocked in Configure Security → Security Policies → FW+IPS Policies.

For the AM-IPS 3500 series Top Layer recommends the following actions:

From the Application Library, add the following applications to the other applications group.

Name	Transport	Port
TCP 139	TCP	139
UDP 139	UDP	139
TCP 445	TCP	445
UDP 445	UDP	445

Note: It is essential that you correctly identify legitimate services that are using the ports described above before implementing a block rule or the services could be impacted inadvertently. If a Service does not exist, use Configure Security → Services → Add Service to create it. Then, add the Service to a list of services to be blocked in Configure Security → Security Policies → FW+IPS Policies.

3. Under Attack Mitigation Settings, select Application Blocking and configure to add the new applications.

4. Add each application and select From outside as the blocking direction.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	http://www.toplayer.com/support
Microsoft Security Bulletin Summary for August 2006	http://www.microsoft.com/technet/security/bulletin/ms06-aug.msp

Relevant TLN Rules: tln-101052