

TopResponse Threat Advisory

Release Date: August 11, 2006

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides additional information needed to block attacks targeting the Microsoft Windows Server Service Buffer Overflow Vulnerability (CVE-2006-3439, MS06-040).

Top Layer Products: IPS 5500 Version 3.40 and higher.

Vulnerable Infrastructure: Microsoft Windows 2000 SP4, Microsoft Windows XP SP1 and SP2, Microsoft Windows XP Professional x64 Edition, Microsoft Windows Server 2003 and Microsoft Windows Server 2003 SP1, 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: Critical Vulnerability

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems using a publicly available exploit

Advisory Impact: Prevention

Summary: The Microsoft Windows Server Service supports sharing of local resources, including files, printers, and named pipes over the network. The reported vulnerability could allow a remote attacker to take complete control of a vulnerable system by sending a specially crafted RPC call using one of the following two ports: TCP/139 or TCP/445.

Recommended Action: Top Layer recommends the following actions:

TopResponse Update Manager™ Users: Download and apply Protection Pack 2006-08-10-06 (or later) to put this new protection into place. No further action is needed.

IPS 5500 Manual Configuration Instructions:

Note: There are different instructions for IPS 5500 Version 3.40 and Version 4.X.

Instructions for Version 3.40:

Version 3.40 users should complete the following steps:

1. Log into the Web Management Interface of your IPS 5500.
2. Select **IPS Configuration->Filter Configuration->Application Protocols->MSNET->RPC->Services->Stub Length**.
3. Click the **Add** button.
4. Enter the following for the new entry:
UUID:
4b324fc8-1670-01d3-1278-5a47bf6ee188
Operation number:
31
Stub Limit:
2
5. Click the **Done** button.
6. Click the **Close** button.
7. Click the **Save** button.

Instructions for Version 4.X:

Version 4.X users should complete the following steps:

1. Log into the Web Management Interface of your IPS 5500.
2. Select **Configure Security->Advanced Security Config->IPS Rules Customization->Protocol Validation Module->MSNET->RPC->Services->Stub Length**.
3. Click the **Add** button.
4. Enter the following for the new entry:
UUID:
4b324fc8-1670-01d3-1278-5a47bf6ee188
Operation number:
31
Stub Limit:
2
5. Click the **Done** button.
6. Click the **Close** button.
7. Click the **Save** icon (upper left of your GUI).

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/ms06-040.msp

Relevant TLN Rules: TLN-008033

Relevant TopResponse Protection Pack(s): 2006-08-10-06