

TopResponse Threat Advisory

Release Date: April 16, 2007

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides additional information needed to block attacks targeting the Microsoft Windows DNS Server RPC Vulnerability (CVE-2007-1748) using another attack vector, as described in the Microsoft advisory update released on 04/15/2007.

Top Layer Products: IPS 5500 Version 3.40 and higher.

Vulnerable Infrastructure: Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Datacenter Server, Microsoft Windows 2000 Server, Microsoft Windows Server 2003 Datacenter Edition, Microsoft Windows Server 2003 Enterprise Edition, Microsoft Windows Server 2003 Standard Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Server 2003 Storage Server.

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 DNS component provides name resolution services for networks. The component can be accessed using the DNS server RPC interface. The reported vulnerability could allow a remote attacker to take complete control of a vulnerable system by sending a specially crafted RPC call containing an escaped sequence of characters as the zone name string argument.

New information shows that this vulnerability can be exploited on TCP 445.

Recommended Action: Top Layer recommends the following actions:

Apply the recommended actions from the previous TopResponse Threat Advisory associated with this vulnerability also issued on April 16, 2007. For TopResponse™ users this consists of downloading and applying Protection Pack 2007-04-16-03 (or later); for others, ensure that the manual configuration instructions have been applied.

Now apply the following additional manual configuration:

IPS 5500 Manual Configuration Instructions:

Note: There are different instructions for IPS 5500 Version 3.40 and Version 4.X. Please make sure that the protection instructions for your version of the IPS 5500 provided in the original Microsoft DNS RPC advisory released earlier have been applied.

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->Groups and Services->Services**
3. Search for the service with the following name:
msdstcp://any:445
4. Select the service.
5. Click the **Edit** button.
6. Click the **Advanced** button.
7. Set the "Process As" setting to:
TCP-DCERPC
8. Click the **OK** button.
9. Click the **OK** button.
10. Click the **Close** button.
11. 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->Security Policies->Services**.
3. Search for the service with the following name:
msds/tcp445
4. Select the service.
5. Click the **Edit** button.
6. Click the **Advanced** button.
7. Set the "Process As" setting to:
MSRPC
8. Click the **OK** button.
9. Click the **OK** button.
10. 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/advisory/935964.mspx

Relevant TLN Rules: TLN-008006, TLN-008007.

Relevant TopResponse Protection Pack(s): 2007-04-16-03