

TopResponse Threat Advisory

Release Date: December 17, 2010.

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Netlogon RPC Null Dereference Denial-of-Service Vulnerability (MS10-101,CVE-2010-2742).

Top Layer Products: IPS 5500 x4.X and higher

Vulnerable Infrastructure: Microsoft Windows Server 2003 Service Pack 2, Microsoft Windows Server 2003 x64 Edition Service Pack 2, Microsoft Windows Server 2003 with SP2 for Itanium-based Systems, Microsoft Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2, Microsoft Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2, Microsoft Windows Server 2008 R2 for x64-based Systems, and other software versions as described in the Microsoft bulletin for the vulnerability.

Alert Type: Critical Vulnerabilities

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to perform a Denial-of-Service attack

Advisory Impact: Prevention

Summary: Microsoft LAN Manager Library (NETAPI) functions can be used to access a Microsoft network. There exists a vulnerability in the NETAPI RPC interface implementation. The reported vulnerability could allow an authenticated attacker to reboot a domain controller system by sending a specially crafted Microsoft RPC request.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2010-12-14-01 (or later) to put this new protection into place. This will put into place protection for the Microsoft Netlogon RPC Null dereference Denial-of-Service Vulnerability that will be applied to the "Recommended Client Protection" and "Recommended Server Protection" IPS Rule Sets.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rules tln-008005 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft NETAPI domain controller infrastructure.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/bulletin/ms10-101.msp

Relevant TLN Rules: tln-008005.

Relevant TopResponse Protection Pack(s): 2010-12-14-01