

TopResponse Threat Advisory

Release Date: April 15, 2010

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against the Microsoft SMTP Server MX Record Vulnerability (MS10-024, CVE-2010-0024).

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

Vulnerable Infrastructure: Microsoft Windows 2000 SP4, Windows XP SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 x64 Edition SP2, Windows Server 2003 SP2 for Itanium-based, Microsoft Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems SP2, Microsoft Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems SP2, and Windows Server 2008 R2 for x64-based Systems, as well as Microsoft Exchange Server 2003 SP2.

Alert Type: Denial of Service

Risk Assessment: High

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to crash the system repeatedly.

Advisory Impact: Prevention

Summary: Microsoft Windows Simple Mail Transfer Protocol (SMTP) component has an error in the handling of specially crafted DNS Mail Exchanger (MX) resource records. The vulnerability can be exploited by sending an unauthenticated packet to a system running the SMTP service. The resulting corruption will cause the service to be unresponsive until restarted. The IPS 5500 provides proactive protection for this vulnerability.

Recommended Action: Top Layer recommends the following actions:

Ensure that the rule tln-101047, "PROTO: DNS Inbound Resource Record Data Contains Invalid Character", is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft systems that have the SMTP service enabled. The rule is currently enabled in the "Recommended Client Protection" and "Recommended Server Protection" IPS Rule Sets.

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/MS10-024.msp
Mitre CVE Advisory	http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0024

Relevant TLN Rules: tln-101047