

TopResponse Threat Advisory

Release Date: October 16, 2008

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Windows Message Queuing Vulnerability (MS08-065,CVE-2008-3479).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Windows 2000 SP4.

Alert Type: Critical vulnerability

Risk Assessment: Critical

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

Advisory Impact: Prevention

Summary: Microsoft Windows Message Queuing (MSMQ) provides message exchange functionality for applications. MSMQ is implemented to support delayed and message exchange such that the sending application can deposit a message for the receiving application to be retrieved at a later time. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the context of the logged-on user by sending a specially crafted DCE-RPC request.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2008-10-14-04 (or later) to put this new protection into place. This is automatically applied to the “Recommended Client Protection” and “Recommended Server Protection” IPS Rule Sets. In order to take advantage of the protection, make sure the IPS rule tln-106203 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft Windows Message Queuing infrastructure.

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/MS08-065.mspx

Relevant TLN Rules: tln-106203

Relevant TopResponse Protection Pack(s): 2008-10-14-04