

TopResponse Threat Advisory

Release Date: April 27, 2010

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block known attacks of the Microsoft Media Services ConnectFunnel Overflow Vulnerability (MS10-025, CVE-2010-0478).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Windows Media Unicast Service in Media Services for Microsoft Windows 2000 Server 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: The Microsoft Media Services is an optional component for installation on Windows 2000 Server. The Unicast service allows selected media to be streamed to a single client. The vulnerability exists in connecting network clients to the server. This could allow an attacker to execute arbitrary code on a user system, where the Microsoft Media Unicast Service is installed and enabled, by sending a specially crafted network packet.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2010-04-23-02 (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-025109 is enabled in the IPS Rule Set used to inspect traffic sent to Microsoft Windows 2000 systems in your infrastructure.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support	http://www.toplayer.com/support
Microsoft Support	http://www.microsoft.com/technet/security/Bulletin/MS10-025.msp
Mitre CVE	http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0478

Relevant TLN Rules: tln-025109

Relevant TopResponse Protection Pack(s): 2010-04-23-02