

TopResponse Threat Advisory

Release Date: December 31, 2010

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Microsoft Windows Movie Maker DLL Hijacking Remote Code Execution (MS10-093,CVE-2010-3967) and Microsoft Windows Media Encoder DLL Hijacking Remote Code Execution (MS10-094,CVE-2010-3965) Vulnerabilities.

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

Vulnerable Infrastructure: Microsoft Windows Movie Maker (WMM) v2.6; Microsoft Windows Media Encoder v9 running on Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, and Windows Server 2008 Gold and SP2.

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 Windows Media Encoder and Microsoft Windows Movie Maker software are vulnerable to DLL Hijacking attacks. The reported vulnerability could allow a remote attacker to execute arbitrary code on the systems running the Microsoft Windows Media Encoder and Microsoft Windows Movie Maker software by enticing a user on the systems to visit a specially crafted web site that causes vulnerable systems to attempt to download a file from an external system using either the WebDAV or the Microsoft RPC protocol. The IPS 5500 provides proactive protection against known attacks targeting the vulnerability.

Recommended Action: Top Layer recommends the following actions:

Ensure that the rule tln-102004, “AAUPV: HTTP Method Name Matches Specified Filter”, is enabled in the IPS Rule Set that is used to inspect traffic sent from your Microsoft Windows Media Encoder and Microsoft Windows Movie Maker infrastructure. The rule is currently enabled in the “Strict Server Protection” IPS Rule Set.

Note: IPS rule tln-102004 is currently enabled in the Strict IPS Rule Set because there is a potential for false positive events. Please monitor events after the rule is enabled to provide protection for this vulnerability.

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/MS10-093.msp |
| Microsoft Advisory | http://www.microsoft.com/technet/security/Bulletin/MS10-094.msp |

Relevant TLN Rules: tln-102004.