



Securing Tomorrow's
Networks Today

TopResponse Threat Advisory

Release Date: April 19, 2010

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide new protection for the Microsoft Directshow MPEG Audio Decoder Stack Overflow Vulnerability (MS10-026, CVE-2010-0480).

Top Layer Products: IPS 5500 E-Series

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, as well as, Microsoft Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems 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 MPEG Layer-3 audio codecs are libraries used by Microsoft Directshow to translate AVI media files save in that format. The vulnerability targets how Microsoft Directshow handles memory when the MPEG Layer-3 audio codecs are utilized. The vulnerability could allow a remote attacker to execute arbitrary code on the client system in the context of the logged-on user by enticing the user to open a specially crafted AVI media file.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2010-04-16-05 (or later) to put this new protection into place. This is automatically applied to the "Strict Client Protection" IPS Rule Set. In order to take advantage of the protection, customers should make sure the IPS rule tln-106312, "EXPLT: Microsoft Directshow MPEG Audio Decoder Stack Overflow Vulnerability", is enabled in the IPS Rule Set used to inspect traffic that transfers AVI media files to your client infrastructure.

Note: The IPS rule tln-106312 is currently enabled in the Strict IPS Rule Sets because there is a potential for false positive events. Please monitor events after the rule is enabled to provide protection for this vulnerability.

To manually enable this rule in a IPS Rule Set complete the following steps:

1. Log into the Web Management Interface of your IPS 5500 E-Series.
 2. Select **Configure Security->Security Policies**.
 3. Select the **IPS Rule Sets** tab.
 4. Select the Rule Set for which you want to change the setting of rule tln-106312.
 5. Enter **tln-106312** in the search window.
 6. Double click on the rule **tln-106312 EXPLT: Microsoft Directshow MPEG Audio Decoder Stack Overflow Vulnerability**.
 7. Make sure that the **Enabled** button is checked.
 8. Make sure that the **Action** is set to **DROP**.
 9. Click the **OK** button.
- Repeat steps 4 through 9 for all other Rule Sets that you want to change.
10. Close the Configure Security Policies window.
 11. Click the **Save** icon (upper left of your GUI).

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/MS10-026.msp
Mitre CVE	http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0480

Relevant TLN Rules: tln-106312

Relevant TopResponse Protection Pack(s): 2010-04-13-05