

TopResponse Threat Advisory

Release Date: October 14, 2009

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide new protection for attacks targetting the Microsoft Windows Media Player Heap Overflow Vulnerability (MS09-052, CVE-2009-2527).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Windows Media Player 6.4 on Microsoft Windows 2000 SP4, Microsoft Windows XP SP2 and SP3, Microsoft Windows XP Professional x64 Edition SP2, Microsoft Windows 2003 SP2, and Microsoft Windows Server 2003 x64 Edition 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: Microsoft Media Player is a default application utilized by Windows to render media content on the system. The reported vulnerability targets how the Media Player engine handles the playback of media files in the ASF format. 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 ASF file hosted on a web page or server.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2009-10-14-02 (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, make sure the IPS rule tln-106276 is enabled in the IPS Rule Set used to inspect traffic that transfers HTML formatted content to your client infrastructure.

Note: The IPS rule tln-106276 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-106276.
 5. Enter **106276** in the search window.
 6. Double click on the rule **tln-106276 EXPLT: Microsoft Windows Media Player Heap 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 Advisory	http://www.microsoft.com/technet/security/Bulletin/MS09-052.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2527

Relevant TLN Rules: tln-106276

Relevant TopResponse Protection Pack(s): 2009-10-14-02