

## TopResponse Threat Advisory

**Release Date:** March 8, 2011

**Purpose:** The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Microsoft Directshow (MS11-015, CVE-2011-0032), Microsoft Groove (MS11-016, CVE-2010-3146), and Microsoft Remote Desktop Insecure Library Loading (MS11-017, CVE-2011-0029) Vulnerabilities.

**Top Layer Products:** IPS 5500 and higher.

### **Vulnerable Infrastructure:**

CVE-2011-0032 - Windows Vista and Vista x64 Service Packs 1 and 2, Windows 7 (32 bit and x64 bit) Service Pack 1, Windows Server 2008 R2 and R2 Systems Service Pack 1 (both for x64), Windows Media Center TV Pack for Windows Vista (32 bit and x64 bit).

CVE-2010-3146 - Microsoft Groove 2007 Service Pack 2.

CVE-2011-0029 - Remote Desktop Connection 5.2 Client, Remote Desktop Connection 6.0 Client and Remote Desktop Connection 6.1 Client, Remote Desktop Connection 7.0 Client, operating system software versions as specified in the Microsoft advisory for the vulnerability.

**Alert Type:** Critical vulnerabilities

**Risk Assessment:** Important

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

**Advisory Impact:** Prevention

**Summary:** A remote code execution vulnerability exists in the way that Microsoft DirectShow, Microsoft Groove, and Windows Remote Desktop Client handles the loading of DLL files. They are vulnerable to DLL Hijacking. The reported vulnerabilities could allow a remote attacker to execute arbitrary code on the systems running these programs by enticing a user on the systems to visit an untrusted remote file system location or WebDAV share and attempt to download a file. The IPS 5500 provides proactive protection against known attacks targeting these vulnerabilities.

**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 to your Microsoft DirectShow, Microsoft Groove, and Windows Remote Desktop Client 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 rules are enabled to provide protection for this vulnerability.

**References:** Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
Microsoft Advisory	<a href="http://www.microsoft.com/technet/security/bulletin/MS11-015.msp">http://www.microsoft.com/technet/security/bulletin/MS11-015.msp</a>
Microsoft Advisory	<a href="http://www.microsoft.com/technet/security/Bulletin/MS11-016.msp">http://www.microsoft.com/technet/security/Bulletin/MS11-016.msp</a>
Microsoft Advisory	<a href="http://www.microsoft.com/technet/security/Bulletin/MS11-017.msp">http://www.microsoft.com/technet/security/Bulletin/MS11-017.msp</a>

**Relevant TLN Rules:** tln-102004.