

## TopResponse Threat Advisory

**Release Date:** March 17, 2010.

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Windows Media DVR-MS Vulnerability (MS11-015,CVE-2011-0042).

**Top Layer Products:** IPS 5500 E-Series.

**Vulnerable Infrastructure:** Microsoft Windows XP Media Center Edition 2005 SP3, Microsoft Windows XP SP3, Microsoft Windows XP Professional x64 Edition SP2, Microsoft Windows Vista SP1 and Windows Vista SP2, Microsoft Windows Vista x64 Edition SP1, Microsoft Windows Vista x64 Edition SP2, Microsoft Windows 7 for 32-bit Systems and Windows 7 for 32-bit Systems SP1, Microsoft Windows 7 for x64-based Systems and Windows 7 for x64-based SP1, Microsoft Windows Media Center TV Pack for Windows Vista, 32-bit editions, Microsoft Windows Media Center TV Pack for Windows Vista, 64-bit editions.

**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 Digital Video Recording (DVR-MS) is an audio and video container format used to store content recorded by Microsoft Windows XP Media Center Edition, Microsoft Windows Vista, and Microsoft Windows 7. There exists a vulnerability in the way Microsoft Windows Media Player and Microsoft Windows Media Center parse DVR-MS files. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the context of the logged-on user by enticing the user to open a specially crafted DVR-MS file.

**Recommended Action:** Top Layer recommends the following actions:

Download and apply Protection Pack 2011-03-16-02 (or later) to put this new protection into place. This will put into place protection for the Microsoft Windows Media DVR-MS Vulnerability that will be applied to the “Recommended Client Protection” IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rule tln-106351 is enabled in the IPS Rule Set used to

inspect traffic to your Microsoft Windows Media Player and Microsoft Windows Media Center infrastructure.

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

| Additional Information | Location  |
|------------------------|---|
| Top Layer Support      | <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> |

**Relevant TLN Rules:** tln-106351.

**Relevant TopResponse Protection Pack(s):** 2011-03-16-02.