

TopResponse Threat Advisory

Release Date: May 17, 2010.

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Powerpoint Presentation Buffer Overrun Vulnerability (MS11-036,CVE-2011-1270).

Top Layer Products: IPS 5500 E-Series:

- 5X software versions V5.31.004 and higher
- 6X software versions V6.10.001 and higher

Vulnerable Infrastructure: Microsoft Office XP SP3, Microsoft Office 2003 SP3, Microsoft Office 2007 SP2, Microsoft Office 2004 for Mac, Microsoft Office 2008 for Mac, Open XML File Format Converter for Mac, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats 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 Powerpoint contains a vulnerability in the way layouts are processed. 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 web site.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2011-05-16-01 (or later) to put this new protection into place. This will put into place protection for the Microsoft Powerpoint Presentation Buffer Overrun 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-106361 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft Powerpoint infrastructure.

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/ms11-036.msp

Relevant TLN Rules: tln-106361.

Relevant TopResponse Protection Pack(s): 2011-05-16-01.