



Securing Tomorrow's
Networks Today

TopResponse Threat Advisory

Release Date: November 10, 2010.

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft PowerPoint Parsing Buffer Overflow Vulnerability (MS10-088,CVE-2010-2572), and the Microsoft PowerPoint Integer Underflow Vulnerability (MS10-088,CVE-2010-2573).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure:

CVE-2010-2572 Microsoft Office PowerPoint 2002 SP3 and 2003 SP3.

CVE-2010-2573 Microsoft PowerPoint 2002 SP3 and 2003 SP3, Office 2004 for Mac , and PowerPoint Viewer 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 is a presentation application that is used to display graphics, formatted text, videos and other media on pre-arranged slides.

CVE-2010-2572 There is a vulnerability in the processing of the Microsoft PPT file format specific to certain PowerPoint 95 files.

CVE-2010-2573 There is a vulnerability in the processing of the Microsoft PowerPoint file format.

In both cases 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 PowerPoint file which was attached to an email or downloaded directly from the network.

Recommended Action: Top Layer recommends the following actions:

CVE-2010-2572 Download and apply Protection Pack 2010-11-09-02 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" IPS Rule Set. In order to take advantage of the protection, customers should make sure the IPS rule tln-106338 is enabled

in the IPS Rule Set used to inspect client traffic that may contain PowerPoint documents.

CVE-2010-2573 Download and apply Protection Pack 2010-11-10-01 (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-106339 is enabled in the IPS Rule Set used to inspect client traffic that may contain PowerPoint documents.

Note: IPS rule tln-106339 is currently enabled in the Strict IPS Rule Set because there is a potential for false positive events. Please monitor events after the rule is enabled to provide protection for this vulnerability.

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/ms10-088.mspx

Relevant TLN Rules: tln-106338, 106339

Relevant TopResponse Protection Pack(s): 2010-11-09-02, 2010-11-10-01