

TopResponse Threat Advisory

Release Date: May 15, 2009

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide new protection for the Microsoft PowerPoint ExEmbed Memory Corruption Vulnerability (MS09-017, CVE-2009-1129).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Office PowerPoint 2000 SP3, Microsoft Office PowerPoint 2002 SP3 and Microsoft Office PowerPoint 2003 SP3.

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. The slides are stored in the PowerPoint Presentation (PPT) file format. There is a vulnerability in the processing of the Microsoft PPT file format; specifically, the vulnerability involves the process of ExEmbed objects found within the file format. 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 PPT file which was attached to an email or downloaded directly from the network.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2009-05-13-05 (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, make sure the IPS rule tln-106243 is enabled in the IPS Rule Set used to inspect traffic that may contain PowerPoint (PPT) documents.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/bulletin/ms09-017.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1129

Relevant TLN Rules: tln-106243

Relevant TopResponse Protection Pack(s): 2009-05-13-05