

TopResponse Threat Advisory

Release Date: April 06, 2009

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide new protection for known attacks targeting the Microsoft PowerPoint Textbox Parsing Vulnerability (CVE-2009-0556).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Office PowerPoint 2000 SP3, Microsoft Office PowerPoint 2002 SP3, Microsoft Office PowerPoint 2003 SP3, and Microsoft Office 2004 for Mac.

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 parsing of the textbox containers 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.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2009-04-03-03 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" and "Recommended Server Protection" IPS Rule Sets. In order to take advantage of the protection, make sure the IPS rule tln-106234 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/advisory/969136.mspx
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0556

Relevant TLN Rules: tln-106234

Relevant TopResponse Protection Pack(s): 2009-04-03-03