

TopResponse Threat Advisory

Release Date: November 11, 2010.

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Office MSO Large SPID Read AV Vulnerability (MS10-087,CVE-2010-3336).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Office XP Service Pack 3, Microsoft Office 2003 Service Pack 3, Microsoft Office 2007 Service Pack 2, Microsoft Office 2010 (32-bit editions), Microsoft Office 2010 (64-bit editions), Microsoft Office 2004 for Mac, Microsoft Office 2008 for Mac, Microsoft Office for Mac 2011, Open XML File Format Converter 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 Office contains a vulnerability in the way that it parses certain Office files which could trigger memory corruption. 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 Office file.

Recommended Action: Top Layer recommends the following actions:

IPS 5500 E-Series Users:

Download and apply Protection Pack 2010-11-11-01 (or later) to put this new protection into place. This will put into place protection for the Microsoft Office MSO Large SPID Read AV Vulnerability that will be applied to the "Strict Client Protection" IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rule tln-106340 is enabled in the IPS Rule Set used to inspect client traffic that may contain Microsoft Office files.

Note: IPS rule tln-106340 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/ms10-087.msp

Relevant TLN Rules: tln-106340

Relevant TopResponse Protection Pack(s): 2010-11-11-01