



Securing Tomorrow's
Networks Today

TopResponse Threat Advisory

Release Date: January 28, 2011.

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block known attacks targeting the Microsoft Office RTF Stack Buffer Overflow Vulnerability (MS10-087,CVE-2010-3333).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Office XP Service Pack, 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 provides support for a number of different file formats, including Rich Text Format (RTF) files. There is a vulnerability in the way Microsoft Office parses RTF data. 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 RTF document.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2011-01-25-01 (or later) to put this new protection into place. This will put into place protection for the Microsoft Office RTF Stack Buffer Overflow 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-022122 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft Office 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/ms10-087.msp

Relevant TLN Rules: tln-022122.

Relevant TopResponse Protection Pack(s): 2011-01-25-01