

## TopResponse Threat Advisory

**Release Date:** December 19, 2008

**Purpose:** The Top Layer TopResponse team is issuing an advisory which provides information needed to provide protection for the Microsoft Word RTF Stylesheet Vulnerability (MS08-072,CVE-2008-4031).

**Top Layer Products:** IPS 5500 E-Series.

**Vulnerable Infrastructure:** Microsoft Office Word 2000 SP3, Microsoft Office Word 2002 SP3, Microsoft Office Word 2003 SP3, Microsoft Office Word 2007, Microsoft Outlook 2007, Microsoft Office Word SP1, Microsoft Outlook 2007 SP1, Microsoft Office Word Viewer 2003, Microsoft Office Word Viewer 2003 SP3, Microsoft Office Compatibility Packs 2007 and 2007 SP1, Microsoft Works 8.5, Microsoft Office 2004 for Mac, Microsoft Office 2008 for Mac, and Microsoft 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:.** The Rich Text Format (RTF) file format is designed for cross-platform document translation. The RTF file format is an accepted input to a large number of Microsoft applications. Among the vulnerable Microsoft applications listed, Microsoft Office Word and Microsoft Outlook are common to desktop infrastructure. The vulnerability is found in how the Microsoft applications handle multiple stylesheet controls during the import of the RTF file. Delivery of a specially crafted file can be made by an RTF formatted email message, RTF file embedded in a web page, or RTF file attachment. The vulnerability could allow an attached document to execute arbitrary code on the client system in the context of the logged-on user by enticing the user to open a specially crafted RTF file.

**Recommended Action:** Top Layer recommends the following actions:

Download and apply Protection Pack 2008-12-17-02 (or later) to put this new protection into place. Protection for this vulnerability 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-106221 is enabled in the IPS Rule Set used to inspect traffic that may contain RTF documents.

**References:** Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
Microsoft Advisory	<a href="http://www.microsoft.com/technet/security/bulletin/MS08-072.msp">http://www.microsoft.com/technet/security/bulletin/MS08-072.msp</a>
Mitre CVE	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4031">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4031</a>

**Relevant TLN Rules:** tln-106221