

## TopResponse Threat Advisory

**Release Date:** April 16, 2009

**Purpose:** The Top Layer TopResponse team is issuing an advisory which provides information needed to provide protection for the Microsoft Wordpad and Office Text Converter Memory Corruption Vulnerability (MS09-010, CVE-2009-0087).

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

**Vulnerable Infrastructure:** Microsoft Windows 2000 Service Pack 4, Windows XP Service Pack 2, Windows XP Service Pack 3, Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2, Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2, Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2, Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems, Office Software and Components, Microsoft Office Word 2000 Service Pack 3, and Microsoft Office Word 2002 Service Pack 3.

**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 Windows provides native text processing for documents in the Word 6.0 format with the Wordpad application. Microsoft Office applications also have functionality to open Word 6.0 formatted documents. The reported vulnerability targets how Microsoft Word 6.0 documents are converted. The handling of process memory can be manipulated by malformed data. The vulnerability could allow a remote attacker 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 Word 6.0 document.

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

Download and apply Protection Pack 2009-04-16-01 (or later) to put this new protection into place. Protection for this vulnerability 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-106238 “EXPLT: Microsoft Wordpad And Office Text Converter Memory Corruption Vulnerability” is enabled in the IPS Rule Set used to inspect traffic that transfers Microsoft Word document files to your client infrastructure.

**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/MS09-010.msp">http://www.microsoft.com/technet/security/bulletin/MS09-010.msp</a>
Mitre CVE	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0087">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0087</a>

**Relevant TLN Rules:** tln-106238

**Relevant TLN Protection Pack:** 2009-04-16-01