

## TopResponse Threat Advisory

**Release Date:** August 12, 2009

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Office Web Components Buffer Overflow Vulnerability (MS09-043, CVE-2009-1534).

**Top Layer Products:** IPS 5500 E-Series running V5.18.002 (or later).

**Vulnerable Infrastructure:** Microsoft Office XP SP3, Microsoft Office 2000 Web Components SP3, Microsoft Office XP Web Components SP3, Microsoft BizTalk Server 2002, and Microsoft Visual Studio .NET 2003 Service Pack 1.

**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 Microsoft Office Web Components ActiveX Control objects are a set of COM components that enables Microsoft Office users to publish Microsoft Office files, such as Microsoft Excel and Word, to the web. The 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 web page.

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

Download and apply Protection Pack 2009-08-11-01 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" IPS Rule Set. In order to take advantage of the protection, customers should make sure the IPS rule tln-106267 is enabled in the IPS Rule Set used to inspect traffic that transfers HTML traffic to your infrastructure.

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

| <b>Additional Information</b> | <b>Location</b>   |
|-------------------------------|---|
| <b>Top Layer Support</b>      | <a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>   |
| <b>Microsoft Advisory</b>     | <a href="http://www.microsoft.com/technet/security/Bulletin/MS09-043.msp">http://www.microsoft.com/technet/security/Bulletin/MS09-043.msp</a> |
| <b>Mitre CVE</b>              | <a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1534">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1534</a>         |

**Relevant TLN Rules:** tln-106267

**Relevant TopResponse Protection Pack(s):** 2009-08-11-01

**Relevant Top Layer Software Version(s):** V5.18.002 or later