

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 Memory Allocation Vulnerability (MS09-043, CVE-2009-0562).

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

Vulnerable Infrastructure: Microsoft Office XP SP3, Microsoft Office 2003 SP3, Microsoft Office XP Web Components SP3, Microsoft Office 2003 Web Components SP3, Microsoft Office 2003 Web Components SP1 for the 2007 Microsoft Office System, Microsoft Internet Security and Acceleration Server 2004 Standard Edition SP3, Microsoft Internet Security and Acceleration Server 2004 Enterprise Edition SP3, Microsoft Internet Security and Acceleration Server 2006 Standard Edition SP1, Internet Security and Acceleration Server 2006 Enterprise Edition SP1, and Microsoft Office Small Business Accounting 2006.

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 "Strict Client Protection" IPS Rule Set. In order to take advantage of the protection, customers should make sure the IPS rule tln-106266 is enabled in the IPS Rule Set used to inspect traffic that transfers HTML traffic to your infrastructure.

Note: The IPS rule tln-106266 is currently enabled in the Strict IPS Rule Sets because there is a potential for false positive events. Please monitor events after the rule is enabled to provide protection for this vulnerability.

To manually enable this rule in a IPS Rule Set complete the following steps:

1. Log into the Web Management Interface of your IPS 5500 E-Series.
2. Select **Configure Security->Security Policies**.
3. Select the **IPS Rule Sets** tab.
4. Select the Rule Set for which you want to change the setting of rule **tln-106266**.
5. Enter **106266** in the search window.
6. Double click on the rule **tln-106266 EXPLT: Microsoft Office Web Components Memory Allocation Vulnerability**.
7. Make sure that the **Enabled** button is checked.
8. Make sure that the **Action** is set to **DROP**.
9. Click the **OK** button.

Repeat steps 4 through 9 for all other Rule Sets that you want to change.

10. Close the Configure Security Policies window.
11. Click the **Save** icon (upper left of your GUI).

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/MS09-043.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0562

Relevant TLN Rules: tln-106266

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

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