

## TopResponse Threat Advisory

**Release Date:** July 14, 2010.

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Access Accwiz.dll ActiveX Remote Code Execution (MS10-044,CVE-2010-0814) and Microsoft Access ActiveX Remote Code Execution (MS10-044,CVE-2010-1881) Vulnerabilities.

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

**Vulnerable Infrastructure:** Microsoft Office 2003 SP3, 2007 Microsoft Office System Service Pack 1, and 2007 Microsoft Office System Service Pack 2.

**Alert Type:** Critical Vulnerabilities

**Risk Assessment:** Critical

**Threat Impact:** Remotely exploitable vulnerabilities that could allow an attacker to control vulnerable systems

**Advisory Impact:** Prevention

**Summary:** Microsoft Access Wizard Controls library (Accwiz.dll) is a runtime component of Microsoft Office Access. The reported Microsoft Access Accwiz.dll ActiveX Remote Code Execution Vulnerability (MS10-044,CVE-2010-0814) 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 site. In addition to the Microsoft Access Wizard Controls library, Microsoft Office Access offers a collection of ActiveX controls that provided additional functionality. The reported Microsoft Access ActiveX Remote Code Execution Vulnerability (MS10-044,CVE-2010-1881) 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 site.

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

**IPS 5500 E-Series Users:**

Download and apply Protection Pack 2010-07-13-01 (or later) to put this new protection into place. This will put into place protection for

1. The Microsoft Access Accwiz.dll ActiveX Remote Code Execution Vulnerability that will be applied to the “Recommended Client Protection” IPS Rule Set.

2. The Microsoft Access ActiveX Remote Code Execution Vulnerability that will be applied to the “Strict Client Protection” IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rules tln-106322 and tln-106323 are enabled in the IPS Rule Set used to inspect traffic to your web client infrastructure.

**Note:** The IPS rule tln-106323 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-106323.
5. Enter **tln-106323** in the search window.
6. Double click on the rule **tln-106323 EXPLT: Microsoft Access ActiveX Remote Code Execution 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
<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/ms10-044.mspx">http://www.microsoft.com/technet/security/bulletin/ms10-044.mspx</a>

**Relevant TLN Rules:** tln-106322, tln-106323

**Relevant TopResponse Protection Pack(s):** 2010-07-13-01