

TopResponse Threat Advisory

Release Date: June 10, 2009

Purpose: The Top Layer TopResponse team is issuing an advisory which provides information needed to provide protection for the Microsoft Internet Explorer Cross-Domain Information Disclosure Vulnerability (MS09-019, CVE-2007-3091).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Internet Explorer 6 SP1 when installed on Microsoft Windows 2000 SP4, Windows XP SP2 and Windows SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 x64 Edition SP2, and Windows Server 2003 with SP2 for Itanium-based Systems; Internet Explorer 7 for Windows XP SP2 and SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 x64 Edition Service Pack 2, Windows Server 2003 with SP2 for Itanium-based Systems, Windows Vista, Windows Vista SP1 and SP2, Windows Vista x64 Edition, Windows Vista x64 Edition SP1 and SP2, Microsoft Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems SP2, and Windows Server 2008 for x64-based Systems, as well as Windows Server 2008 for x64-based Systems SP2.

Alert Type: Information Disclosure

Risk Assessment: Important

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to read data from other web browser sessions.

Advisory Impact: Prevention

Summary: Microsoft Internet Explorer is a common web browser used by Microsoft client infrastructure to retrieve and render content from the network. The reported vulnerability targets how Microsoft Internet Explorer handles the processing of script objects embedded into a web page that handle the navigation of web pages between domains. Sensitive data in one trusted web session should not be accessible by an attacker in another session originating from an untrusted domain. The vulnerability could allow a remote attacker to read data from other web browser session open on the client system by enticing the user to open a specially crafted web page.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2009-06-10-01 (or later) to put this new protection into place. Protection for this vulnerability is automatically applied to the “Strict Client Protection” IPS Rule Set.

In order to take advantage of the protection, make sure the IPS rule tln-106247 “EXPLT: Microsoft IE Cross-Domain Information Disclosure Vulnerability” is enabled in the IPS Rule Set used to inspect traffic to your Microsoft client infrastructure.

Note: The IPS rule tln-106247 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 any 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 106247
5. Enter **106247** in the search window
6. Double click on the rule **tln-106247 EXPLT: Microsoft IE Cross-Domain Information Disclosure 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 Web site	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/bulletin/MS09-019.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3091

Relevant TLN Rules: tln-106247

Relevant TLN Protection Pack: 2009-06-10-01