

TopResponse Threat Advisory

Release Date: January 15, 2010

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide new protection for the Microsoft Internet Explorer Remote Code Execution Vulnerability (CVE-2010-0249).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Internet Explorer 6 on Microsoft Windows 2000 SP4, Windows XP SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 SP2 for Itanium-based and x64 Edition SP2;

Internet Explorer 7 for Windows XP SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 SP2 for Itanium-based Systems, Windows Server 2003 x64 Edition SP2, Windows Vista SP2, Windows Vista x64 Edition SP2, Windows Server 2008 for 32-bit, Itanium-based, and x64-based Systems SP2;

Internet Explorer 8 for Windows XP SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, and Windows Server 2003 x64 Edition SP2, Windows Vista SP2, Windows Vista x64 Edition SP2, Windows Server 2008 for 32-bit, Itanium-based, and x64-based Systems SP2, Windows 7 for 32-bit and x64-based Systems, and Windows Server 2008 R2 for x64-based and Itanium-based Systems.

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 Internet Explorer is a common web browser used by Microsoft client infrastructure to retrieve and render content from the network. The publicly exploited vulnerability targets how Microsoft Internet Explorer handles an invalid pointer reference after a deleted object is freed from memory. The processing of the invalid memory will crash Internet Explorer. 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 web page.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2010-01-15-02 (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, make sure the IPS rule tln-106291 is enabled in the IPS Rule Set used to inspect traffic that transfers HTML formatted content to your client infrastructure.

Note: The IPS rule tln-106291 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-106291.
5. Enter **tln-106291** in the search window.
6. Double click on the rule **tln-106291 EXPLT: Microsoft Internet Explorer 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:

Information	Location
Top Layer Support	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/advisory/979352.mspx
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249

Relevant TLN Rules: tln-106291

Relevant TopResponse Protection Pack(s): 2010-01-15-02