

TopResponse Threat Advisory

Release Date: April 15, 2009

Purpose: The Top Layer TopResponse team is issuing an advisory which provides information needed to provide protection for the Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability (MS09-014, CVE-2009-0553).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Internet Explorer v6 SP1 running on Windows 2000 SP4; Microsoft Internet Explorer v6 running on Windows XP SP2 / SP3, Windows Server 2003 SP1 / SP2, Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition SP2, Windows Server 2003 with SP1 / SP2 for Itanium-based Systems; Internet Explorer v7 running on Windows XP SP2 / SP3, Windows Server 2003 SP1 / SP2, Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition SP2, Windows Server 2003 with SP1 / SP2 for Itanium-based, Windows Vista and Windows Vista SP1, Windows Vista x64 Edition and Microsoft Windows Vista x64 Edition SP1, Windows Server 2008 for 32-bit Systems, Windows Server 2008 for x64-based Systems, and Windows Server 2008 for 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 reported vulnerability targets how Microsoft Internet Explorer handles the processing of objects embedded into a web page that have not been correctly initialized or have been deleted. 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 2009-04-15-02 (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-106237 “EXPLT: Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability” is enabled in the IPS Rule Set used to inspect traffic to your Microsoft client infrastructure.

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 106237
5. Enter **106237** in the search window
6. Double click on the rule **tln-106237 EXPLT: Microsoft Internet Explorer Uninitialized Memory Corruption 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/MS09-014.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0553

Relevant TLN Rules: tln-106237

Relevant TLN Protection Pack: 2009-04-15-02