

TopResponse Threat Advisory

Release Date: July 14, 2009

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide new protection for the Microsoft Embedded OpenType Font Heap Overflow Vulnerability (MS09-029, CVE-2009-0231).

Top Layer Products: IPS 5500 E-Series

Vulnerable Infrastructure: Microsoft Windows 2000 SP4, Windows XP SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 x64 Edition SP2, Windows Vista SP2, Windows Vista x64 Edition SP2, Windows Server 2008 SP2.

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 Embedded OpenType (EOT) Font engine is a component of the Microsoft Windows Operating System that enables the delivery of custom embedded fonts for use in web content. The author creates a font object and links it within the page that displays a custom font. Upon downloading the EOT object, the browser forwards the content to the Microsoft Embedded OpenType (EOT) Font engine. The vulnerability could allow an attacker to execute arbitrary code on the client systems in the context of the logged-on user by enticing the user to open specially crafted web content.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2009-07-14-06 (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-106264 is enabled in the IPS Rule Set used to inspect traffic that transfers web pages to your client infrastructure.

Note: The IPS rule tln-106264 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-106264.
 5. Enter **106264** in the search window.
 6. Double click on the rule **tln-106264 EXPLT: Microsoft Embedded OpenType Font Heap Overflow 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/ms09-029.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0231

Relevant TLN Rules: tln-106264

Relevant TopResponse Protection Pack(s): 2009-07-14-06