

TopResponse Threat Advisory

Release Date: May 19, 2009

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against the Microsoft IIS WebDAV Authentication Bypass Vulnerability (CVE-2009-1535).

Top Layer Products: IPS 5500 v4.X and higher.

Vulnerable Infrastructure: Microsoft IIS 6.0, Microsoft IIS 5.1 and Microsoft IIS 5.0.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems and replace arbitrary files on the web server.

Advisory Impact: Prevention

Summary: Microsoft Internet Information Server (IIS) is the default web server used by Microsoft server infrastructure. The vulnerability involves the bypass of authentication when WebDAV is used for content publication. By bypassing authentication, an attacker is able to upload and overwrite arbitrary data served by the web server with malicious content. Subsequent visitor to the compromised Microsoft IIS web server will be served the malicious content.

Specific attacks using the Microsoft IIS WebDAV Authentication Bypass vulnerability have emerged and are actively exploiting systems. The IPS 5500 provides proactive protection for this vulnerability.

Recommended Action: Top Layer recommends the following actions:

For IPS 5500 E-Series customers: Ensure that the rule tln-016010, “PROTO: HTML Illegal character found in document body”, is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft IIS 6.0 web server systems that have WebDAV enabled. The rule is currently enabled in the “Strict Client Protection” and “Strict Server Protection” IPS Rule Set.

For IPS 5500 v4.X and higher customer: Ensure that the rule tln-102004, “AAUPV: HTTP Method Name Matches Specified Filter”, is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft IIS 6.0 web server systems that have WebDAV enabled. The rule is currently enabled in the “Strict Server Protection” IPS Rule Sets.

Note: IPS 5500 E-Series customer may see rule tln-102004 events and rule tln-016010 events when both rules are enabled. Rule tln-016010 blocks an additional attack vector for this vulnerability when enabled on a IPS 5500 E-Series.

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.
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-102004
5. Enter **102004** in the search window
6. Double click on the rule **tln-102004 AAUPV: HTTP Method Name Matches Specified Filter**
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).

IPS 5500 E-Series customers should repeat steps 1 through 11 for rule tln-016010 in all Rule Sets that you want to change.

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/advisory/971492.mspx
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1535

Relevant TLN Rules: tln-102004

tln-016010 for E-Series Customers