

TopResponse Threat Advisory

Release Date: June 10, 2009

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against the Microsoft IIS 5.0 WebDAV Authentication Bypass Vulnerability (MS09-020, CVE-2009-1122).

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

Vulnerable Infrastructure: Microsoft IIS 5.0.

Alert Type: Elevation of Privilege

Risk Assessment: Moderate

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to 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 visitors to the compromised Microsoft IIS web server will be served the malicious content. The IPS 5500 provides proactive protection for this vulnerability.

Recommended Action: Top Layer recommends the following actions:

Ensure that the rule tln-102019, "PROTO: HTTP URI Path Contains Invalid Character", is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft IIS 5.0 web server systems that have WebDAV enabled. The rule is currently enabled in the "Strict Server Protection" IPS Rule Set.

Note: The IPS rule tln-102019 is currently enabled in the Strict IPS Rule Sets because there is a potential for false positive events. Please monitor events after these rules are 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.
 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-102019.
 5. Enter **102019** in the search window.
 6. Double click on the rule **tln-102019 PROTO: HTTP URI Path Contains Invalid Character**.
 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/MS09-020.mspx
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1122

Relevant TLN Rules: tln-102019