

TopResponse Threat Advisory

Release Date: December 8, 2008

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection for known attacks targeting the Microsoft Communications Server 2007 SIP INVITE Denial of Service Vulnerability (CVE-2008-5180).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Office Communications Server 2007

Alert Type: Denial of Service Resulting from memory consumption

Risk Assessment: Moderate

Threat Impact: External Denial of Service condition

Advisory Impact: Prevention

Summary: Microsoft Office Communications Server 2007 is a key component of the Microsoft Unified Communications architecture that unites Microsoft Office applications, Active Directory services and existing telephony infrastructure. Microsoft Office Communications Server 2007 manages real-time communications including: instant messaging, VoIP, audio and video conferencing. The reported attacks targeting this Microsoft vulnerability could allow a remote attacker to exhaust available server memory by creating a large number of SIP INVITE requests. The IPS 5500 provides proactive protection for known attacks targeting this vulnerability.

Recommended Action: Top Layer recommends the following actions:

Ensure that the rule tln-020041, "PROTO: SIP Illegal Request Header", is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft Communications Server 2007. This rule is not currently included in the "Recommend" or "Strict" rule sets.

See the following steps for how to enable the rule in a rule set.

IPS 5500 E-Series Manual Configuration Instructions:

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 tln-020041
5. Enter **020041** in the search window
6. Double click on the rule **tln-020041 PROTO: SIP Illegal Request Header**
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
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5180

Relevant TLN Rules: tln-020041