

TopResponse Threat Advisory

Release Date: December 31, 2010

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection for the Microsoft IIS FastCGI Request Header Buffer Overflow Vulnerability (MS10-065,CVE-2010-2730).

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

Vulnerable Infrastructure: Microsoft Internet Information Services v7.5 with FastCGI enabled.

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: The Microsoft Internet Information Services (IIS) web server contains support for the FastCGI protocol. The protocol is an alternative to the Common Gateway Interface (CGI) protocol that offers better performance, improved reliability, and a more efficient environment for non-thread safe application frameworks than the CGI protocol. The reported vulnerability could allow a remote attacker to execute arbitrary code on the systems running the Microsoft IIS web server with FastCGI support by sending a number of specially crafted HTTP headers in an HTTP request. The IPS 5500 provides proactive protection for the vulnerability.

Recommended Action: Top Layer recommends the following actions:

Ensure that the rule tln-102054, “AAUPV: HTTP Message Contains Too Many Headers”, is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft IIS server infrastructure. The rule is currently enabled in the “Recommended Client Protection” and “Recommended Server Protection” IPS Rule Sets.

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/MS10-065.mspx

Relevant TLN Rules: tln-102054.