

TopResponse Threat Advisory

Release Date: August 17, 2007

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against attacks on the Microsoft VML CDownloadSink VGX.DLL Vulnerability (CVE-2007-1749).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Internet Explorer v5.01, v6, v6 SP1, and v7.

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 VGX.DLL is a component used to render Vector Markup Language (VML) documents. The reported vulnerability could allow a remote attacker to execute arbitrary code on a vulnerable system by enticing a user to visit or open a specially crafted web page containing a link to compressed content on an attacker-controlled web site. The IPS 5500 provides proactive protection against the vulnerability.

Recommended Action: Top Layer recommends the following actions:

1. Install the updated version of the Microsoft VML component, as described in the Microsoft Security Bulletin MS07-050.
2. Ensure that the rule tln-016014, "EXPLT: Microsoft Internet Explorer VML Overflow Vulnerability", is enabled. This rule is enabled by default in the "Recommended Client Protection", and the "Recommended Server Protection" 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/ms07-050.aspx

Relevant TLN Rules: TLN-016014.