

TopResponse Threat Advisory

Release Date: November 12, 2008

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block attacks targeting the Microsoft XML IFRAME Memory Corruption Vulnerability (MS08-069, CVE-2007-0099).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft XML Core Services v3.0

Alert Type: Critical vulnerability

Risk Assessment: Important

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems

Advisory Impact: Prevention

Summary: The Microsoft XML Core Services v3.0 is a system component that provides XML translation for web browsers and software applications. Typical examples of applications that utilize the Microsoft XML Core Services v3.0 are Internet Explorer and the Microsoft Office suite of applications. The vulnerability is located in the msxml3.dll library XML parsing functions. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the context of the logged-on user by enticing the user to open a specially crafted web page or HTML email.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2008-11-11-06 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" IPS Rule Set.

In order to take advantage of the protection, make sure the IPS rule tln-106210 is enabled in the IPS Rule Sets used to inspect traffic to your Microsoft client infrastructure.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	http://www.toplayer.com/support
Mitre CVE Bulletin	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0099
Microsoft Security Bulletin	http://www.microsoft.com/technet/security/bulletin/ms08-069.msp

Relevant TLN Rules: tln-106210

Relevant TopResponse Protection Pack(s): 2008-11-11-06