

TopResponse Threat Advisory

Release Date: February 15, 2008

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block attacks for the Microsoft OLE Heap Overrun Vulnerability (CVE-2007-0065).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP1 and SP2, Vista, Office 2004 for Mac, and Visual basic 6.0 SP6.

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: Microsoft Object Linking and Embedding (OLE) Automation is a protocol that allows an application to share data with or control another application. There is a vulnerability in the OLE automation component that can be exploited using an ActiveX control. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the security context of the logged-on user by enticing the user to open a specially crafted web page.

Recommended Action: Top Layer recommends the following actions:

IPS 5500 E-Series Users: Download and apply Protection Pack 2008-02-13-02 (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-106176 is enabled in the IPS Rule Set used to inspect traffic from your client infrastructure.

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/ms08-008.msp

Relevant TLN Rules: tln-106176

Relevant TopResponse Protection Pack(s): 2008-02-13-02