

TopResponse Threat Advisory

Release Date: July 14, 2009

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Office Web Components Remote Code Execution ActiveX Vulnerability (CVE-2009-1136).

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

Vulnerable Infrastructure: Microsoft Office XP SP3, Microsoft Office 2003 SP3, Microsoft Office XP Web Components SP3, Microsoft Office 2003 Web Components SP3, Microsoft Office 2003 Web Components for the 2007 Microsoft Office system SP1, Microsoft Internet Security and Acceleration Server 2004 Standard Edition SP3, Microsoft Internet Security and Acceleration Server 2004 Enterprise Edition SP3, Microsoft Internet Security and Acceleration Server 2006, Internet Security and Acceleration Server 2006 Supportability Update, Microsoft Internet Security and Acceleration Server 2006 SP1, and Microsoft Office Small Business Accounting 2006.

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 Office Web Components ActiveX Control objects are a set of COM components that enables Microsoft Office users to publish Microsoft Office files, such as Microsoft Excel and Word, to the web. The 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.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2009-07-14-01 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" and "Recommended Server Protection" IPS Rule Sets. In order to take advantage of the protection, customers should make sure the IPS rule tln-106263 is enabled in the IPS Rule Set used to inspect traffic that transfers HTML traffic to your 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/advisory/973472.mspx
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1136

Relevant TLN Rules: tln-106263

Relevant TopResponse Protection Pack(s): 2009-07-14-01