

TopResponse Threat Advisory

Release Date: October 31, 2008

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block attacks targeting the Microsoft Office Web Components Spreadsheet (MS08-017,CVE-2006-4695), Microsoft Office Web Components DataSourceControl (MS08-017,CVE-2007-1201), and the PhotoStockPlus Uploader Tool (CVE-2008-0957) Vulnerabilities.

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Office Web Components (OWC) 2000, Microsoft BizTalk Server 2000, Microsoft BizTalk Server 2002, Microsoft Commerce Server 2000, Microsoft Internet Security and Acceleration Server 2000, Microsoft Office 2000, Microsoft Office XP, Microsoft Visual Studio .NET 2002, Microsoft Visual Studio .NET 2003; PhotoStockPlus Uploader Tool v1.0.

Alert Type: Critical vulnerabilities

Risk Assessment: Moderate

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

Advisory Impact: Prevention

Summary: Microsoft Office Web Components (OWC) are a group of OLE classes implemented as ActiveX controls. Applications such as Microsoft Excel, Access and FrontPage can create interactive web pages using Office Web Components. The PhotoStockPlus Uploader Tool can be used to upload images to a web site. The reported vulnerabilities in OWC and PhotoStockPlus Uploader Tool 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 web page. Microsoft provided an update for these vulnerabilities as part of the Microsoft Cumulative Security Update on October 29, 2008.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2008-10-30-03 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" and "Recommended Server Protection" IPS Rule Set. In order to take advantage of the protection for the Microsoft Office Web Components Vulnerabilities, make sure the IPS rules tln-106205 and tln-106206 are enabled in the IPS Rule Sets used to inspect traffic to your

Microsoft Office Web Components client infrastructure. In order to take advantage of the protection provided for the PhotoStockPlus Uploader Tool, make sure the IPS rule tln-106207 is enabled in the IPS Rule Set used to inspect traffic to your PhotoStockPlus Uploader Tool client infrastructure.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support Web site	http://www.toplayer.com/support
Microsoft Cumulative Security Update	http://www.microsoft.com/technet/security/advisory/956391.mspx

Relevant TLN Rules: tln-106205, tln-106206, tln-106207

Relevant TopResponse Protection Pack(s): 2008-10-30-03