

TopResponse Threat Advisory

Release Date: December 9, 2008

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide protection for various Microsoft Visual Basic ActiveX controls. The provided protection includes the following controls: MSDataGrid ObjText ActiveX Vulnerability (MS08-070,CVE-2008-4252), FlexGrid FormatString ActiveX Vulnerability (MS08-070,CVE-2008-4253), MSHierarchicalFlexGridLib ObjRows ActiveX Vulnerability (MS08-070,CVE-2008-4254), MSChart DoSetCursor ActiveX Vulnerability (MS08-070,CVE-2008-4256) and Animation Object Vulnerability (MS08-070,CVE-2008-4255).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Visual Basic 6.0 Runtime Extended Files; Microsoft Visual Studio .NET 2002 Service Pack 1; Microsoft Visual Studio .NET 2003 Service Pack 1; Microsoft Visual FoxPro 8.0 Service Pack 1; Microsoft Visual FoxPro 9.0 Service Pack 1; Microsoft Visual FoxPro 9.0 Service Pack 2; Microsoft Office FrontPage 2002 Service Pack 3; Microsoft Office Project 2003 Service Pack 3; Microsoft Office Project 2007 Service Pack 1

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: Components from Visual Basic 6 are utilized and redistributed with products built using this development environment. The various ActiveX Control for Visual Basic 6 are also available in other development environments, such as Microsoft .Net and Microsoft FoxPro. The reported vulnerabilities target these Microsoft ActiveX controls. Each vulnerability could allow an attacker to execute arbitrary code on the client system 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 2008-12-09-03 (or later) to put this new protection into place.

The protection for these vulnerabilities is detailed in the table below.

Protection for most vulnerabilities is automatically applied to the "Recommended Client Protection" and "Recommended Server Protection" IPS Rule Sets. The exception is rule tln-106218 which will take effect when the "Strict Client Protection" IPS Rule Set is applied. In order to take advantage of the protection, make sure the IPS rule tln-106214 through tln-106218 are enabled in the IPS Rule Set used to inspect traffic is sent to your Microsoft client infrastructure.

Rule ID	CVE ID	Description	Client	Server
tln-106214	CVE-2008-4252	MSDataGrid ObjText	Recommended	Recommended
tln-106214	CVE-2008-4253	FlexGrid FormatString	Recommended	Recommended
tln-106216	CVE-2008-4254	MSHierarchicalFlexGridLib	Recommended	Recommended
tln-106217	CVE-2008-4256	MSChart DoSetCursor	Recommended	Recommended
tln-106218	CVE-2008-4255	Animation Object	Strict	--

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/MS08-070.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4252 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4253 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4254 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4255 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4256

Relevant TLN Rules: tln-106214 through tln-106218