

TopResponse Threat Advisory

Release Date: October 14, 2009

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft ATL COM Initialization Vulnerability (MS09-055, CVE-2009-2493).

Top Layer Products: IPS 5500 E-Series running V5.18.002 (or later).

Vulnerable Infrastructure: Microsoft Windows 2000 SP4, Windows XP SP2 and SP3, Windows XP Professional x64 Edition SP2, Windows Server 2003 SP2, Windows Server 2003 x64 Edition SP2, Windows Server 2003 with SP2 for Itanium-based Systems, Windows Vista SP1 and SP2, Windows Vista x64 Edition SP1 and SP2, Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2, Windows Server 2008 for x64-based Systems SP2, Windows Server 2008 for Itanium-based Systems SP2, Windows 7 for 32-bit Systems, Windows 7 x64 Edition, Windows Server 2008 R2 for x64-based Systems, as well as Windows Server 2008 R2 for Itanium-based Systems.

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 Active Template Library (ATL) is a set of ActiveX Control objects that are used in products such as the Office Web Components, Outlook View Controls, Windows Live Mail Components, Visio Viewer, and MSN Photo Upload Tool. 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 2009-10-14-02 (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, customers should make sure the IPS rule tln-106275 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	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/Bulletin/MS09-055.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2493

Relevant TLN Rules: tln-106275

Relevant TopResponse Protection Pack(s): 2009-10-14-02

Relevant Top Layer Software Version(s): V5.18.002 or later