

TopResponse Threat Advisory

Release Date: July 6, 2009

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Video ActiveX Vulnerability (CVE-2008-0015).

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

Vulnerable Infrastructure: Microsoft Windows XP Service Pack 2, Windows XP Service Pack 3, Windows XP Professional x64 Edition Service Pack 2, Windows Server 2003 Service Pack 2, Windows Server 2003 x64 Edition Service Pack 2, and Windows Server 2003 with SP2 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 Video Control object is an ActiveX component that enables Microsoft Windows Media Center to DirectShow filters for recording and playing television video. 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 2009-07-06-02 (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-106260 is enabled in the IPS Rule Set used to inspect traffic that transfers HTML traffic to your infrastructure.

In Protection Pack 2009-07-06-02 (or later), the SANS_DSshield blocked IP address list has been updated to provide protection against post-exploitation attempts by known exploits of the reported vulnerability. Ensure that your IPS Unit's Security Policy table contains a policy row configured to block traffic to or from the SANS_DSshield Host Group.

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/972890.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0015

Relevant TLN Rules: tln-106260

Relevant TopResponse Protection Pack(s): 2009-07-06-02