

TopResponse Threat Advisory

Release Date: April 15, 2011.

Purpose: The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide proactive protection for the Microsoft WMI Administrative Tools Remote Code Execution Vulnerability (MS11-027,CVE-2010-3973).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft WMI Tools ActiveX control in WBEMSingleView.ocx 1.50.1131.0 in Microsoft WMI Administrative Tools 1.1 and earlier in Microsoft Windows XP SP2 and SP3.

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: Microsoft Windows Management Instrumentation (WMI) Tools include the Managed Object Format (MOF) compiler, the WMI administrative tools, the WMI tester tool, and other tools. Microsoft Internet Explorer implements support for access to the WMI tools, including the WMI Administrative tools. There is a vulnerability in the way one of the methods of the WMI Administrative ActiveX component is implemented. The reported 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 site. The IPS 5500 provides proactive protection for this vulnerability.

Recommended Action: Top Layer recommends the following actions:

Ensure that the rule tln-022124, “EXPLT: Microsoft WMI Administrative Tools Remote Code Execution Vulnerability”, is enabled in the IPS Rule Set used to inspect traffic that transfers HTML traffic to your infrastructure which may have the vulnerable tool set installed. The rule is currently enabled in the “Recommended Client Protection” IPS Rule Set.

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/MS11-027.msp

Relevant TLN Rules: tln-022124.

Relevant TopResponse Protection Pack(s): 2011-02-17-01.