

TopResponse Threat Advisory

Release Date: April 11, 2008

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block attacks for the Microsoft Internet Explorer (IE) hxvz.dll ActiveX Vulnerability (CVE-2008-1086).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Internet Explorer 5.01 SP4 on Microsoft Windows 2000 SP4; Internet Explorer 6 SP1 on Microsoft Windows 2000 SP4; Windows XP SP2, Windows XP Professional x64 Edition, Windows XP Professional x64 Edition SP2, Windows Vista, Windows Vista SP1, Windows Vista x64 Edition, and Windows Vista x64 Edition SP1.

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 IE offers access to various ActiveX controls. There is a vulnerability in the ActiveX controls corresponding to the Microsoft IE hxvz.dll component. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the security 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 2008-04-08-01 (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, make sure the IPS rule tln-106184 is enabled in the IPS Rule Set used to inspect traffic from your client infrastructure.

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/MS08-023.msp |

Relevant TLN Rules: tln-106184

Relevant TopResponse Protection Pack(s): 2008-04-08-01