

## TopResponse Threat Advisory

**Initial Release Date:** July 17, 2008

**Updated Release:** August 15, 2008 – Added reference to Microsoft Bulletin

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to block attacks targeting the Microsoft Snapshot Viewer ActiveX Vulnerability (CVE-2008-2463).

**Top Layer Products:** IPS 5500 E-Series.

**Vulnerable Infrastructure:** Microsoft Access Snapshot Viewer 11.0.8164.0 and prior, Microsoft Access Snapshot Viewer 10.0.6515.0 and prior; Microsoft Access 2000, Microsoft Access 2002, Microsoft Access 2003, Microsoft Office 2000, Microsoft Office XP, Microsoft Office 2003.

**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 Snapshot Viewer is a tool that can be used to view Microsoft Access files without a full license. The tool is used in combination with the Microsoft Access Report Snapshot utility to generate portable reports. 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 2008-07-14-02 (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, make sure the IPS rule tln-106194 is enabled in the IPS Rule Set used to inspect traffic from your Microsoft Access client infrastructure.

**References:** Use the following sources for additional information:

Additional Information	Location
<b>Top Layer Support Web site</b>	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
<b>Microsoft Advisory</b>	<a href="http://www.microsoft.com/technet/security/advisory/955179.msp">http://www.microsoft.com/technet/security/advisory/955179.msp</a>
<b>Microsoft Bulletin</b>	<a href="http://www.microsoft.com/technet/security/bulletin/ms08-041.msp">http://www.microsoft.com/technet/security/bulletin/ms08-041.msp</a>

**Relevant TLN Rules:** tln-106194

**Relevant TopResponse Protection Pack(s):** 2008-07-14-02