

## TopResponse Threat Advisory

**Release Date:** March 31, 2009

**Purpose:** The Top Layer TopResponse team informs customers that existing IPS 5500 security features provide new protection for known attacks targeting the Microsoft GDI EMF Filename Parameter Overflow Vulnerability (MS08-021 / CVE-2008-1087).

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

**Vulnerable Infrastructure:** Microsoft Internet Explorer 6 SP1, Microsoft Office 2003, Microsoft Office XP, Microsoft Office System 2007, Microsoft PowerPoint Viewer 2003, Microsoft Report Viewer 2005 SP1 Redistributable Package, Microsoft Report Viewer 2008 Redistributable Package, Microsoft SQL Server 2000 Reporting Services SP2, Microsoft SQL Server 2005, Microsoft Visio 2002 SP2, Microsoft Windows 2000, Microsoft Windows Vista, Microsoft Windows XP, Microsoft Windows Sever 2003, Microsoft Windows Sever 2008, Microsoft Works 8.0, Microsoft Digital Image Suite 2006, Microsoft Forefront Client Security 1.0.

**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 GDI+ enables applications to use graphics and formatted text on both the video display and the printer. One of the file formats defined by Microsoft that can directly access the GDI+ subsystem API is the Extended MetaFile (EMF) file format. There is a vulnerability in the implementation of the Microsoft GDI+ parser for the EMF file format; specifically, the vulnerability involves the process of parsing of the filename parameter in the EMF file format. 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 EMF file.

**Recommended Action:** Top Layer recommends the following actions:

Download and apply Protection Pack 2009-03-30-02 (or later) to put this new protection into place. This is automatically applied to the “Strict Client Protection” and “Strict Server Protection” IPS Rule Sets. In order to take advantage of the protection, make sure the IPS rule tln-022113 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft GDI+ client infrastructure.

**Note:** The IPS rule tln-022113 is currently enabled in the Strict IPS Rule Sets because there is a potential for false positive events. Please monitor events after the rule is enabled to provide protection for this vulnerability.

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

Additional Information	Location
Top Layer Support Web site	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
Microsoft Advisory	<a href="http://www.microsoft.com/technet/security/bulletin/MS08-021.mspx">http://www.microsoft.com/technet/security/bulletin/MS08-021.mspx</a>
Mitre CVE	<a href="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1087">http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1087</a>

**Relevant TLN Rules:** tln-022113

**Relevant TopResponse Protection Pack(s):** 2009-03-30-02