

TopResponse Threat Advisory

Release Date: September 17, 2008

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection against attacks targeting Microsoft GDI+ Vulnerabilities using the RSClientPrint vector (MS08-052, CVE-2007-5348, CVE-2008-3012, CVE-2008-3013, CVE-2008-3014, CVE-2008-3015).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Internet Explorer v6, Microsoft .NET Framework v1.0, Microsoft .NET Framework v1.1 SP1, Microsoft .NET Framework v2.0, Microsoft .NET Framework v2.0 SP1; Microsoft Office XP SP3, Microsoft Office 2003 SP2, Microsoft Office XP SP3, Microsoft Office 2007, Microsoft Office 2007 SP1, Microsoft Office Project 2002 SP2, Microsoft Visio 2002 SP2, Microsoft Office Word Viewer, Microsoft Office Powerpoint Viewer 2003, Microsoft Office Excel Viewer, Microsoft Works 8, Microsoft Digital Image Suite 2006.

Alert Type: Critical vulnerability

Risk Assessment: Moderate

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. There are several vulnerabilities in the way Microsoft GDI+ handles memory allocation, parses images, and certain parameters. One of the vectors that can be used to exploit the vulnerabilities is by instantiating the RSClientPrint control in Internet Explorer. This 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 web page.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2008-09-11-01 (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-106200 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft GDI+ 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/ms08-052.msp?pubDate=2008-09-09

Relevant TLN Rules: tln-106200

Relevant TopResponse Protection Pack(s): 2008-09-11-01