



Securing Tomorrow's
Networks Today

TopResponse Threat Advisory

Release Date: January 17, 2010.

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to block known attacks targeting the Microsoft Graphics Rendering Engine CreateSizedDibSection Vulnerability (CVE-2010-3970).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Windows XP SP3, Microsoft Windows XP Professional x64 Edition SP2, Microsoft Windows Server 2003 SP2, Microsoft Windows Server 2003 x64 Edition SP2, Microsoft Windows Server 2003 with SP2 for Itanium-based Systems, Microsoft Windows Vista Service Pack 1 and Windows Vista SP2, Microsoft Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition SP2, Microsoft Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems SP2, Microsoft Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems SP2, Microsoft Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems SP2.

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 Graphics Rendering Engine (GRE) implements functions capable of processing thumbnails. One of these functions contains a vulnerability in the way bitmaps are processed. 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 Microsoft Office document.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2011-01-14-03 (or later) to put this new protection into place. This will put into place protection for the Microsoft Graphics Rendering Engine CreateSizedDibSection Vulnerability that will be applied to the "Recommended Client Protection" IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rule tln-025118 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft Graphics Rendering Engine infrastructure.

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/advisory/2490606.msp

Relevant TLN Rules: tln-025118.

Relevant TopResponse Protection Pack(s): 2011-01-14-03