

TopResponse Threat Advisory

Release Date: November 23, 2009

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for known attacks targeting the Microsoft Win32k EOT Parsing Vulnerability (MS09-065,CVE-2009-2514).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Windows 2000 SP4; Windows XP SP2 and SP3; Windows XP Professional x64 Edition SP2; Windows Server 2003 SP2; Windows Server 2003 x64 Edition SP2; Windows Server 2003 with SP2 for Itanium-based Systems; Windows Vista SP1 and SP2; Windows Vista x64 Edition SP1 and SP2; Windows Server 2008 for 32-bit Systems SP2; Windows Server 2008 for x64-based Systems SP2; 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 Embedded OpenType (EOT) fonts are a portable font description file format for use in web pages. There is a kernel-mode remote code execution exploit in the way that Microsoft Windows parses the EOT file format records. The vulnerability could allow a remote attacker to execute arbitrary code on the client system in the context of the logged-on user by enticing the user to open a specially crafted EOT file embedded on a web page or server. Default settings on Microsoft Windows typically does not prompt users when downloading and loading this file type.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2009-11-23-01 (or later) to put this new protection into place. This is automatically applied to the "Recommended Client Protection" and "Recommended Server Protection" IPS Rule Sets. In order to take advantage of the protection, customers should make sure the IPS rule tln-106284 is enabled in the IPS Rule Set used to inspect traffic that transfers EOT files to your 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/Bulletin/MS09-065.msp
Mitre CVE	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2514

Relevant TLN Rules: tln-106286

Relevant TopResponse Protection Pack(s): 2009-11-23-01