

TopResponse Threat Advisory

Release Date: December 19, 2011.

Purpose: The Corero TopResponse team informs customers that existing IPS 5500 security features provide proactive protection against known attacks targeting the Microsoft Win32k TrueType Font Parsing Vulnerability (MS11-087,CVE-2011-3402).

Corero Products: Corero IPS 5500 and later.

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 SP2, Microsoft Windows Vista x64 Edition SP2, Microsoft Windows Server 2008 for 32-bit Systems SP2, Microsoft Windows Server 2008 for x64-based Systems SP2, Microsoft Windows Server 2008 for Itanium-based Systems SP2, Microsoft Windows 7 for 32-bit Systems and Microsoft Windows 7 for 32-bit Systems SP1, Microsoft Windows 7 for x64-based Systems and Microsoft Windows 7 for x64-based Systems SP1, Microsoft Windows Server 2008 R2 for x64-based Systems and Microsoft Windows Server 2008 R2 for x64-based Systems SP1, Microsoft Windows Server 2008 R2 for Itanium-based Systems, and Microsoft Windows Server 2008 R2 for Itanium-based Systems SP1.

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 kernel contains Win32k.sys (Win32k), a kernel-mode device driver that controls window displays, manages screen output, and passes user messages to applications. There exists a vulnerability in the Win32k device driver's font parsing routines. The reported vulnerability could allow a remote attacker to execute arbitrary code on the vulnerable infrastructure components by enticing users to open a specially crafted TTF file. The IPS 5500 provides proactive protection against known attacks targeting this vulnerability.

Recommended Action: Corero recommends the following actions:

Ensure that the rule tln-106398, "EXPLT: Microsoft Win32k TrueType Font Parsing Vulnerability", is enabled in the IPS Rule Set that is used to inspect traffic sent to your Microsoft Internet Explorer infrastructure. The rule is currently enabled in the "Recommended Client Protection" IPS Rule Set.

References: Use the following sources for additional information:

Additional Information	Location
Corero Support	https://support.corero.com/
Microsoft Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms11-087

Relevant IPS 5500 Rules: tln-106398.