

TopResponse Threat Advisory

Release Date: November 7, 2011.

Purpose: The Corero TopResponse team is issuing an advisory, which provides information needed to block known attacks targeting the Microsoft Win32k TrueType Font Parsing Vulnerability (CVE-2011-3402).

Corero Products: Top Layer IPS 5500 E-Series 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 Win32k TrueType parsing engines contains a vulnerability in the way TrueType font types are handled. 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 TrueType font type.

Recommended Action: Corero recommends the following actions:

Download and apply Protection Pack 2011-11-07-03 (or later) to put this new protection into place. This will put into place protection against known attacks targeting the Microsoft Win32k TrueType Font Parsing 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-106398 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft infrastructure.

References: Use the following sources for additional information:

Additional Information	Location
Corero Support	http://www.corero.com/support
Microsoft Advisory	http://technet.microsoft.com/en-us/security/advisory/2639658

Relevant IPS 5500 Rules: tln-106398.

Relevant TopResponse Protection Pack(s): 2011-11-07-03.