

Threat Update Service* Advisory
Protection Pack 2013-05-28-01 Released May 28, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Microsoft Windows Win32k Font Parsing Vulnerability.

Issue: The Windows kernel-mode driver does not properly handle font files. This could allow an attacker to cause a denial of service of the system until it is restarted by enticing the victim to open a specially crafted website.

Recommended Action: Apply the specified protection pack (or any later one) and ensure the associated rule is used to inspect traffic to the affected product infrastructure.

| | |
|----------------------------|---|
| Issue Identifier | CVE-2013-1291, MS13-036 |
| Advisory | http://technet.microsoft.com/en-us/security/bulletin/ms13-036 |
| Risk Assessment | Important Vulnerability |
| Threat Impact | Remotely exploitable vulnerability that could allow an attacker to cause a denial of service of an unprotected system. |
| Affected Products | Windows XP Windows Server 2003 Windows Vista Windows Server 2008 Windows 7 Windows 8 |
| Corero Products | IPS 5500 E-Series and later. |
| Associated Rule | tln-106627 |
| Associated Rule Set | This rule is automatically enabled in the "Recommended Client Protection" rule set. |

* previously called TopResponse

<https://support.corero.com> Corero Network Security, Inc.
One Cabot Road, Hudson, MA 01749 +1 978.212.1500 • Fax +1 978.212.1600
• USA • Japan • Asia Pacific • EMEA Copyright 2013. All Rights Reserved.