

## Threat Update Service\* Advisory

### Protection Pack 2013-10-10-03 Released October 11, 2013

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft Windows CVE-2013-3128 OpenType Font Parsing Vulnerability.

**Issue:** Microsoft Windows does not properly parse OpenType fonts (OTF) thereby corrupting system memory. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted file. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

**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.

<b>Issue Identifier</b>	CVE-2013-3128, MS13-081, MS13-082
<b>Advisory</b>	<a href="http://technet.microsoft.com/en-us/security/bulletin/ms13-081">http://technet.microsoft.com/en-us/security/bulletin/ms13-081</a> <a href="http://technet.microsoft.com/en-us/security/bulletin/ms13-082">http://technet.microsoft.com/en-us/security/bulletin/ms13-082</a>
<b>Risk Assessment</b>	Critical Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
<b>Affected Products</b>	Windows XP Service Pack 3 Windows XP Professional x64 Edition Service Pack 2 Windows Server 2003 Service Pack 2 Windows Vista Service Pack 2 Windows Vista x64 Edition Service Pack 2 Windows Server 2008 for 32-bit and 64-bit Systems Service Packs 1 and 2 Windows 7 for 32-bit and 64-bit Systems Service Pack 1 Windows Server 2008 R2 for x64-based and Itanium-based Systems Service Pack 1 Windows 8 for 32-bit and 64-bit Systems Windows Server 2012 Windows RT Windows Server 2012 (Server Core installation)
<b>Corero Products</b>	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
<b>Associated Rule</b>	tln-106721
<b>Associated Rule Set</b>	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.