

Threat Update Service* Advisory

Protection Pack 2012-12-14-02 Released December 14, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft Windows CVE-2012-4786 TrueType Font Parsing Vulnerability.

Issue: Microsoft Windows font parsing does not properly handle objects in memory when parsing TrueType Font files. This could allow an attacker to execute arbitrary code on the victim's machine. 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.

| | |
|----------------------------|--|
| Issue Identifier | CVE-2012-4786, MS12-078 |
| Vendor Advisory | http://technet.microsoft.com/security/bulletin/MS12-078 |
| Risk Assessment | Critical Vulnerability |
| Threat Impact | Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system. |
| Affected Products | Windows XP Windows Server 2003 Windows Vista Windows 7 Windows Server 2008 (including Server Core installation) Windows 8 Windows Server 2012 (including Server Core installation) Windows RT |
| Corero Products | IPS 5500 E-Series and later. |
| Associated Rule | tln-106561 |
| Associated Rule Set | This rule is automatically enabled in the "Strict 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 2012. All Rights Reserved.