

Threat Update Service* Advisory

Protection Pack 2014-10-15-01 Released October 15, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft Windows CVE-2014-4148 TTF Parsing Vulnerability.

Issue: Windows kernel-mode driver does not properly handle TrueType fonts. This could allow an attacker to execute arbitrary code on the victim’s machine by enticing the victim to open a specially crafted website. 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-2014-4148, MS14-058
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms14-058
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Windows Server 2003 Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8 and Windows 8.1 Windows Server 2012 and Windows Server 2012 R2 Windows RT and Windows RT 8.1
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later), v6.82 (build 003 and later).
Associated Rule	tIn-106948
Associated Rule Set	This rule is automatically enabled in the “Strict Client Protection” rule set.

* previously called TopResponse

<http://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 2014. All Rights Reserved.