

Threat Update Service* Advisory
Protection Pack 2013-11-01-03 Released November 4, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Kingsoft Writer WPS Font Names Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in the Kingsoft Writer. This could allow a remote attacker to execute arbitrary code on the vulnerable machine via a long font name in a WPS 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.

Issue Identifier	CVE-2013-3934
Advisory	http://www.securityfocus.com/bid/61796
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Kingsoft Writer 2012 8.1.0.3030 Kingsoft Office 2013 before 9.1.0.4256
Corero Products	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).
Associated Rule	tIn-022185
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.