Threat Update Service* Advisory

Protection Pack 2013-11-13-04 Released November 13, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft Word CVE-2013-1324 Stack Buffer Overwrite Vulnerability.

Issue: A stack buffer overflow vulnerability exists in Microsoft Office. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted WordPerfect document (.wpd) 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-2013-1324, MS13-091
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms13-091
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Microsoft Office 2003 SP3, 2007 SP3, 2010 SP1 and SP2, 2013, and 2013 RT
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	tln-106739
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