

Threat Update Service* Advisory

Protection Pack 2012-12-11-03 Released December 11, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft Word RTF listoverridecount Remote Code Execution Vulnerability.

Issue: Microsoft Office does not properly handle memory when parsing RTF files. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted RTF 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-2012-2539, MS12-079
Vendor Advisory	http://technet.microsoft.com/security/bulletin/MS12-079
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 Word 2003 Service Pack 3 Microsoft Word 2007 Service Packs 2 and 3 Microsoft Word 2010 Service Pack 1 (32-bit and 64-bit editions) Microsoft Word Viewer Microsoft Office Compatibility Pack Service Packs 2 and 3 Microsoft Office Web Apps 2010 Service Pack 1
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106555
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 2012. All Rights Reserved.