

## Threat Update Service\* Advisory

### Protection Pack 2014-11-12-01 Released November 12, 2014

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft Office CVE-2014-6333 Remote Code Execution Vulnerability.

**Issue:** Microsoft Word improperly handles objects in memory thereby corrupting system memory. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted document. 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.

<b>Issue Identifier</b>	CVE-2014-6333, MS14-069
<b>Advisory</b>	<a href="http://technet.microsoft.com/en-us/security/bulletin/ms14-069">http://technet.microsoft.com/en-us/security/bulletin/ms14-069</a>
<b>Risk Assessment</b>	Critical Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
<b>Affected Products</b>	Microsoft Word 2007 Service Pack 3 Microsoft Word Viewer Microsoft Office Compatibility Pack Service Pack 3
<b>Corero Products</b>	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).
<b>Associated Rule</b>	tlN-106965
<b>Associated Rule Set</b>	This rule is automatically enabled in the "Recommended 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.