

**Threat Update Service\* Advisory**  
**Protection Pack 2015-02-13-01 Released February 13, 2015**

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Microsoft Office CVE-2015-0064 Remote Code Execution Vulnerability.

**Issue:** Microsoft Office 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-2015-0064, MS15-012
<b>Advisory</b>	<a href="https://technet.microsoft.com/library/security/ms15-012">https://technet.microsoft.com/library/security/ms15-012</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 Office 2010 Service Pack 2
<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-107043
<b>Associated Rule Set</b>	This rule is automatically enabled in the "Recommended Client Protection" rule set.

\* previously called TopResponse