

## Threat Update Service\* Advisory June 11, 2013

**Purpose:** The Corero Security Active Response Team informs customers that the IPS 5500 has proactive coverage against potential attacks targeting the Microsoft Office Buffer Overflow Vulnerability.

**Issue:** Microsoft Office does not properly allocate memory when parsing PNG files. This could allow an attacker to execute arbitrary code on the victim's machine and possibly take complete control of an affected system.

**Recommended Action:** Enable the specified rule and ensure that the rule is used to inspect traffic to the affected product infrastructure.

<b>Issue Identifier</b>	CVE-2013-1331, MS13-051
<b>Advisory</b>	<a href="https://technet.microsoft.com/en-us/security/bulletin/ms13-051">https://technet.microsoft.com/en-us/security/bulletin/ms13-051</a>
<b>Risk Assessment</b>	Important Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
<b>Affected Products</b>	Microsoft Office 2003 Service Pack 3 Microsoft Office for Mac 2011
<b>Corero Products</b>	IPS 5500 E-Series and later.
<b>Associated Rule</b>	tln-012018
<b>Associated Rule Set</b>	This rule is automatically enabled in the "Recommended Client Protection" and "Strict Server Protection" rule sets.

\* 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.