

**Threat Update Service\* Advisory**  
**Protection Pack 2013-05-28-01 Released May 28, 2013**

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft Visio CVE-2013-1301 XML External Entities Resolution Vulnerability.

**Issue:** Microsoft Visio does not properly parse XML files containing external entities that are resolved within other XML external entity declarations. This could allow an attacker to gain access to sensitive information by enticing the victim to open a specially crafted Visio document.

**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-2013-1301, MS13-044
<b>Advisory</b>	<a href="http://technet.microsoft.com/en-us/security/bulletin/ms13-044">http://technet.microsoft.com/en-us/security/bulletin/ms13-044</a>
<b>Risk Assessment</b>	Important Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to gain access to sensitive information on an unprotected system.
<b>Affected Products</b>	Microsoft Visio 2003 Service Pack 3 Microsoft Visio 2007 Service Pack 3 Microsoft Visio 2010 Service Pack 1 (32-bit and 64-bit editions)
<b>Corero Products</b>	IPS 5500 E-Series and later.
<b>Associated Rule</b>	tlN-106625
<b>Associated Rule Set</b>	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 2013. All Rights Reserved.