

## **Threat Update Service\* Advisory**

### **Protection Pack 2013-01-18-01 Released January 18, 2013**

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Adobe Acrobat and Reader CVE-2012-1530 Memory Corruption Vulnerability.

**Issue:** A memory corruption vulnerability exists in Adobe Reader and Acrobat. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted PDF 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-2012-1530
<b>Vendor Advisory</b>	<a href="http://www.adobe.com/support/security/bulletins/apsb13-02.html">http://www.adobe.com/support/security/bulletins/apsb13-02.html</a>
<b>Identified In</b>	January 2013 Adobe Patch Tuesday release
<b>Risk Assessment</b>	Critical 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>	Adobe Reader and Acrobat 9.x before 9.5.3 Adobe Reader and Acrobat 10.x before 10.1.5 Adobe Reader and Acrobat 11.x before 11.0.1
<b>Corero Products</b>	IPS 5500 E-Series and later.
<b>Associated Rule</b>	tln-106568
<b>Associated Rule Set</b>	This rule is automatically enabled in the "Strict 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.