

## Threat Update Service\* Advisory

### Protection Pack 2014-01-23-01 Released January 23, 2014

**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-2014-0496 Use-After-Free Vulnerability.

**Issue:** A use-after-free vulnerability exists in Adobe Reader and Acrobat. This could allow an attacker to execute arbitrary code on the affected system via a specially crafted PDF 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-2014-0496
<b>Advisory</b>	<a href="http://helpx.adobe.com/security/products/acrobat/apsb14-01.html">http://helpx.adobe.com/security/products/acrobat/apsb14-01.html</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>	Adobe Reader and Acrobat 10.x before 10.1.9 and 11.x before 11.0.06 on Windows and Mac OS X
<b>Corero Products</b>	IPS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.62 (build 007 and later), v6.80 (build 035 and later).
<b>Associated Rule</b>	tln-106775
<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 2014. All Rights Reserved.