

**Threat Update Service\* Advisory**  
**Protection Pack 2014-01-08-02 Released January 9, 2014**

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Adobe Reader CVE-2013-3346 ToolButton Use-After-Free Vulnerability.

**Issue:** A remote code execution vulnerability exists in Adobe Reader and Acrobat. This could allow an attacker to execute arbitrary code on the victim's machine via a specially crafted PDF file.

**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-2013-3346
<b>Advisory</b>	<a href="http://www.adobe.com/support/security/bulletins/apsb13-15.html">http://www.adobe.com/support/security/bulletins/apsb13-15.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 9.x before 9.5.5 Adobe Reader and Acrobat 10.x before 10.1.7 Adobe Reader and Acrobat 11.x before 11.0.03
<b>Corero Products</b>	IPS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
<b>Associated Rule</b>	tIn-022190
<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.