

**Threat Update Service\* Advisory**  
**Protection Pack 2013-11-25-01 Released November 25, 2013**

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Adobe Reader CVE-2013-3353 Code Execution Vulnerability.

**Issue:** A buffer overflow 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 file. 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-2013-3353
<b>Advisory</b>	<a href="http://www.adobe.com/support/security/bulletins/apsb13-22.html">http://www.adobe.com/support/security/bulletins/apsb13-22.html</a>
<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 before 10.1.8 and 11.x before 11.0.04 on Windows and Mac OS X
<b>Corero Products</b>	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
<b>Associated Rule</b>	tln-106751
<b>Associated Rule Set</b>	This rule is automatically enabled in the “Recommended Client Protection” rule set.

\* previously called TopResponse