

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

### **Protection Pack 2013-02-08-02 Released February 8, 2013**

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Adobe Flash Player CVE-2013-0634 Memory Corruption Vulnerability.

**Issue:** A memory corruption vulnerability exists in Adobe Flash Player. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted SWF 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-2013-0634
<b>Vendor Advisory</b>	<a href="http://www.adobe.com/support/security/bulletins/apsb13-04.html">http://www.adobe.com/support/security/bulletins/apsb13-04.html</a>
<b>Identified In</b>	February 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 Flash Player 11.5.502.146 and earlier versions for Windows and Macintosh Adobe Flash Player 11.2.202.261 and earlier versions for Linux Adobe Flash Player 11.1.115.36 and earlier versions for Android 4.x Adobe Flash Player 11.1.111.31 and earlier versions for Android 3.x and 2.x
<b>Corero Products</b>	IPS 5500 E-Series and later.
<b>Associated Rule</b>	tln-106580
<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 2012. All Rights Reserved.