

Threat Update Service* Advisory

Protection Pack 2013-03-01-03 Released March 1, 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-2013-0648 Remote Code Execution Vulnerability.

Issue: A remote code execution 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 specially crafted SWF content. 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.

Issue Identifier	CVE-2013-0648
Vendor Advisory	http://www.adobe.com/support/security/bulletins/apsb13-08.html
Identified In	February 2013 Adobe release
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Adobe Flash Player before 10.3.183.67 and 11.x before 11.6.602.171 on Windows and Mac OS X Adobe Flash Player before 10.3.183.67 and 11.x before 11.2.202.273 on Linux
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106597
Associated Rule Set	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.