

Threat Update Service* Advisory

Protection Pack 2012-12-14-02 Released December 14, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Adobe Flash Player and AIR CVE-2012-5676 Remote Buffer Overflow Vulnerability.

Issue: A buffer overflow vulnerability exists in Adobe Flash Player and Adobe AIR. 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.

Issue Identifier	CVE-2012-5676
Vendor Advisory	http://www.adobe.com/support/security/bulletins/apsb12-27.html
Identified In	December 2012 Adobe Patch Tuesday 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 10.3.183.48 Adobe Flash Player 11.x before 11.5.502.135 on Windows Adobe Flash Player 11.x before 11.5.502.136 on Mac OS X Adobe Flash Player 11.x before 11.2.202.258 on Linux Adobe Flash Player before 11.1.111.29 on Android 2.x and 3.x Adobe Flash Player before 11.1.115.34 on Android 4.x Adobe AIR before 3.5.0.880 on Windows Adobe AIR before 3.5.0.890 on Mac OS X Adobe AIR SDK before 3.5.0.880 on Windows Adobe AIR SDK before 3.5.0.890 on Mac OS X
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106557
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.