Threat Update Service* Advisory

Protection Pack 2012-10-11-02 Released October 12, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Adobe Flash Player CVE-2012-4171 Remote Code Execution Vulnerability.

Issue: A memory corruption 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-2012-4171
Vendor Advisory	http://www.adobe.com/support/security/bulletins/apsb12-19.html
Identified In	August 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 10.x before 10.3.183.23 on Windows and Mac OS X Adobe Flash Player 11.x before 11.4.402.265 on Windows and Mac OS X Adobe Flash Player 10.x before 10.3.183.23 on Linux Adobe Flash Player 11.x before 11.2.202.238 on Linux Adobe Flash Player before 11.1.111.16 on Android 2.x and 3.x Adobe Flash Player before 11.1.115.17 on Android 4.x Adobe AIR before 3.4.0.2540 Adobe AIR SDK before 3.4.0.2540
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106525
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