Threat Update Service* Advisory

Protection Pack 2014-02-25-03 Released February 25, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Adobe Flash Player CVE-2014-0498 Remote Code Execution Vulnerability.

Issue: A stack buffer overflow vulnerability exists in the Adobe Flash Player. This could allow an attacker to execute arbitrary code on the affected system via a specially crafted SWF file.

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-2014-0498
Advisory	http://helpx.adobe.com/security/products/flash-player/apsb14-07.html
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Adobe Flash Player before 11.7.700.269 Adobe Flash Player 11.8.x through 12.0.x before 12.0.0.70 on Windows and Mac OS X Adobe Flash Player before 11.2.202.341 on Linux Adobe AIR before 4.0.0.1628 on Android Adobe AIR SDK before 4.0.0.1628 Adobe AIR SDK & Compiler before 4.0.0.1628
Corero Products	IPS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.62 (build 007 and later), v6.80 (build 035 and later).
Associated Rule	tln-106804
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