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-2013-0633 Buffer Overflow Vulnerability.

Issue: A buffer overflow 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 Word document containing malicious 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-2013-0633
Vendor Advisory	http://www.adobe.com/support/security/bulletins/apsb13-04.html
Identified In	February 2013 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 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
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106579
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