Threat Update Service* Advisory

Protection Pack 2012-08-17-02 Released August 17, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Adobe Flash Player Embedded OpenType Font 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-2012-1535
Vendor Advisory	http://www.adobe.com/support/security/bulletins/apsb12-18.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 before 11.3.300.271 on Windows and Mac OS X Adobe Flash Player before 11.2.202.238 on Linux
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106497
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