

Threat Update Service* Advisory
Protection Pack 2013-07-23-01 Released July 24, 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-2013-3345 Memory Corruption Vulnerability.

Issue: A memory corruption 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 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-2013-3345
Advisory	http://www.adobe.com/support/security/bulletins/apsb13-17.html
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 11.7.700.232 on Windows and Mac OS X Adobe Flash Player 11.8.x before 11.8.800.94 on Windows and Mac OS X Adobe Flash Player before 11.2.202.297 on Linux Adobe Flash Player before 11.1.111.64 on Android 2.x and 3.x Adobe Flash Player before 11.1.115.69 on Android 4.x
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tIn-106663
Associated Rule Set	This rule is automatically enabled in the "Strict Client Protection" rule set.

* previously called TopResponse