Threat Update Service* Advisory

Protection Pack 2015-01-19-02 Released January 19, 2015

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Adobe Flash Player CVE-2015-0304 Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in the 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 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-2015-0304
Advisory	http://helpx.adobe.com/security/products/flash-player/apsb15-01.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 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later), v6.82 (build 003 and later).
Associated Rule	tln-025298
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

