Threat Update Service* Advisory

Protection Pack 2014-04-08-02 Released April 8, 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-2014-0509 Cross Site Scripting Vulnerability.

Issue: A cross-site scripting vulnerability exists in the Adobe Flash Player. This could allow an attacker to inject arbitrary web script or HTML in the context of the victim's browser by enticing the victim to open 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-2014-0509
Advisory	http://helpx.adobe.com/security/products/flash-player/apsb14-09.html
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute scripts on an unprotected system.
Affected Products	Adobe Flash Player 12.0.0.77 on Windows
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-106849
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

