

**Threat Update Service\* Advisory**  
**Protection Pack 2015-08-31-01 Released Sept 1, 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-2015-0340 Security Bypass Vulnerability.

**Issue:** A Security Bypass Vulnerability exists in the Adobe Flash Player. This could allow an attacker to bypass intended file-upload restrictions via unspecified vectors.

**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.

<b>Issue Identifier</b>	CVE-2015-0340
<b>Advisory</b>	<a href="https://helpx.adobe.com/security/products/flash-player/apsb15-05.html">https://helpx.adobe.com/security/products/flash-player/apsb15-05.html</a>
<b>Risk Assessment</b>	Critical Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
<b>Affected Products</b>	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux
<b>Corero Products</b>	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).
<b>Associated Rule</b>	tln-025335
<b>Associated Rule Set</b>	This rule is automatically enabled in the "Recommended Server Protection" rule set.

\* previously called TopResponse