

Threat Update Service* Advisory
Protection Pack 2015-11-23-01 Released November 30, 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-2015-3102 Bypass the Same Origin Policy Vulnerability.

Issue: A Security Bypass Vulnerability exists in the Adobe Flash Player. This could allow an attacker to bypass the same-origin-policy and lead to information disclosure.

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-2015-3102 |
| Advisory | https://helpx.adobe.com/security/products/flash-player/apsb15-11.html |
| Risk Assessment | Critical Vulnerability |
| Threat Impact | Remotely exploitable vulnerability that could allow an attacker to bypass the same-origin-policy and lead to information disclosure. |
| Affected Products | 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 |
| 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-025338 |
| Associated Rule Set | This rule is automatically enabled in the "Recommended Server Protection" rule set. |

* previously called TopResponse