

Threat Update Service* Advisory

Protection Pack 2016-05-17-01 Released May 31, 2016

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Adobe Flash Player CVE-2015-3108 Memory Access Vulnerability.

Issue: A Memory Access Vulnerability exists in the Adobe Flash Player. This could allow attackers to bypass the ASLR protection mechanism 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.

Issue Identifier	CVE-2015-3108
Advisory	https://helpx.adobe.com/security/products/flash-player/apsb15-11.html
Risk Assessment	Critical vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow attackers to bypass the ASLR protection mechanism via unspecified vectors.
Affected Products	This Memory Access Vulnerability affects Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors.
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-025343
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse