Threat Update Service* Advisory

Protection Pack 2014-12-22-02 Released December 22, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Adobe Reader and Acrobat CVE-2014-9165 Use After Free Vulnerability.

Issue: A use after free vulnerability exists in the Adobe Reader and Acrobat. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted PDF 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-2014-9165
Advisory	http://helpx.adobe.com/security/products/reader/apsb14-28.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 Reader and Acrobat 10.x before 10.1.13 and 11.x before 11.0.10 on Windows and OS X
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-025295
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

