

Threat Update Service* Advisory

Protection Pack 2014-02-19-01 Released February 19, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Adobe Acrobat And Reader CVE-2014-0493 Remote Code Execution Vulnerability.

Issue: A memory corruption vulnerability exists in the Adobe Reader and Acrobat. This could allow an attacker to execute arbitrary code on the affected system via a specially crafted PDF 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-2014-0493
Advisory	http://helpx.adobe.com/security/products/acrobat/apsb14-01.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 10.1.9 and 11.x before 11.0.06 on Windows and Mac OS X
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-106801
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

<https://support.corero.com> Corero Network Security, Inc.
One Cabot Road, Hudson, MA 01749 +1 978.212.1500 • Fax +1 978.212.1600
• USA • Japan • Asia Pacific • EMEA Copyright 2014. All Rights Reserved.