

Threat Update Service* Advisory

Protection Pack 2013-02-14-04 Released February 14, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Adobe Acrobat and Reader CVE-2013-0641 Remote Code Execution Vulnerability.

Issue: A remote code execution vulnerability exists in 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-2013-0641
Vendor Advisory	http://blogs.adobe.com/psirt/2013/02/adobe-reader-and-acrobat-vulnerability-report.html
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Adobe Reader and Acrobat 9.x through 9.5.3 Adobe Reader and Acrobat 10.x through 10.1.5 Adobe Reader and Acrobat 11.x through 11.0.1
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106590
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 2012. All Rights Reserved.