

Threat Update Service* Advisory
Protection Pack 2013-05-10-03 Released May 10, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Aloaha PDF Crypter ActiveX Arbitrary File Overwrite Vulnerability.

Issue: Aloaha PDF Crypter does not properly validate input to the SaveToFile() method in the vbCrypt.dll ActiveX control thereby allowing a remote attacker to overwrite arbitrary files.

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	BID: 57543
Advisory	http://www.securityfocus.com/bid/57543
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to overwrite arbitrary files on an unprotected system.
Affected Products	PDF Crypter 3.5.0.1164
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106619
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 2013. All Rights Reserved.