Threat Update Service* Advisory

Protection Pack 2012-12-06-04 Released December 6, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Splunk Search Remote Code Execution Vulnerability.

Issue: Splunk Web does not properly restrict use of the mappy command to access Python classes. This could allow a remote authenicated attacker to execute arbitrary code on the victim's machine via a CSRF attack.

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-2011-4642
Advisory	http://www.splunk.com/view/SP-CAAAGMM
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain control of an unprotected system.
Affected Products	Splunk 4.2.x before 4.2.5
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025150
Associated Rule Set	This rule is automatically enabled in the "Recommended Server 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.