

Threat Update Service* Advisory
Protection Pack 2014-05-30-01 Released May 30, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the SPIP CVE-2013-2118 Security Bypass Vulnerability.

Issue: A security bypass vulnerability exists in SPIP. This could allow an attacker to gain elevated privileges and gain control of the system via the 'ecire/inc/filtres.php' script.

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-2013-2118
Advisory	http://contrib.spip.net/SPIP-3-0-9-2-1-22-2-0-23-corrections-de-bug-et-faille?lang=fr
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain elevated privileges on an unprotected system.
Affected Products	SPIP 3.0.x before 3.0.9, 2.1.x before 2.1.22, and 2.0.x before 2.0.23
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-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	tIn-106872
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

<http://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.