

Threat Update Service* Advisory Protection Pack 2014-04-24-06 Released April 25, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Sophos Web Protection Appliance Security Bypass Vulnerability.

Issue: A security bypass vulnerability exists in the Sophos Web Appliance. This could allow an attacker to change the admin password via a specially crafted request.

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-2014-2849
Advisory	http://www.sophos.com/en-us/support/knowledgebase/120230.aspx
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to change the admin password on an unprotected system.
Affected Products	Sophos Web Appliance before 3.8.2
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	tIn-025251
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.