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 Remote Command Execution Vulnerability.

Issue: A remote command execution vulnerability exists in the Sophos Web Appliance. This could allow an attacker to execute arbitrary commands on the victim's machine via shell metacharacters in the address parameter.

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-2014-2850
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 execute arbitrary commands 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	tln-025252
Associated Rule Set	This rule is automatically enabled in the "Strict Server Protection" rule set.

* previously called TopResponse

 Copyright 2014. All Rights Reserved.