Threat Update Service* Advisory

Protection Pack 2013-08-12-05 Released August 12, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Apache Struts 2 Open Redirection Vulnerability.

Issue: An open redirection vulnerability exists in Apache Struts which could allow an attacker to carry out phishing attacks via a URL in a parameter using the redirect: or redirectAction: prefix.

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-2013-2248
Advisory	http://struts.apache.org/release/2.3.x/docs/s2-017.html
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to carry out phishing attacks.
Affected Products	Apache Struts 2.0.0 through 2.3.15
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 013 and later), v6.80 (build 035 and later).
Associated Rule	tln-106667
Associated Rule Set	This rule is automatically enabled in the “Recommended Server Protection” rule set.

* previously called TopResponse

