Threat Update Service* Advisory

Protection Pack 2013-12-03-01 Released December 4, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Apache Struts Parameterinterceptor Class OGNL Security Bypass Vulnerability.

Issue: A security bypass vulnerability exists in Apache Struts. This could allow an attacker to manipulate server-side objects with the privileges of the user running the Apache application and possibly take complete control of the application.

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-2011-3923
Advisory	http://www.securityfocus.com/bid/51628
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to take complete control of the Apache application.
Affected Products	Apache Struts2 before v2.3.1.2
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-021507
Associated Rule Set	This rule is automatically enabled in the “Recommended Server Protection” rule set.

* previously called TopResponse

