Threat Update Service* Advisory

Protection Pack 2014-02-19-01 Released February 19, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Apache Struts ExceptionDelegator Remote Command Execution Vulnerability.

Issue: The ExceptionDelegator component in Apache Struts does not properly validate OGNL expressions during exception handling. This could allow an attacker to execute arbitrary code on the affected system via a specially crafted 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-2012-0391
Advisory	http://struts.apache.org/2.x/docs/version-notes-2311.html
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Apache Struts before 2.2.3.1
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-025234
Associated Rule Set	This rule is automatically enabled in the “Recommended Server Protection” rule set.

* previously called TopResponse

