Threat Update Service* Advisory

Protection Pack 2013-08-15-04 Released August 15, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Apache Struts CVE-2013-2135 OGNL Expression Injection Vulnerability.

Issue: Apache Struts does not validate requests containing both "${}" and "%{}" sequences correctly. This could allow an attacker to execute arbitrary ONGL code on the system via crafted requests.

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-2013-2135
Advisory	http://struts.apache.org/development/2.x/docs/s2-015.html
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code.
Affected Products	Apache Struts 2 before 2.3.14.3
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-106670
Associated Rule Set	This rule is automatically enabled in the “Strict Server Protection” rule set.

* previously called TopResponse

