Threat Update Service* Advisory

Protection Pack 2014-10-10-01 Released October 10, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Apache Struts includeParams CVE-2013-2115 Remote Code Execution Vulnerability.

Issue: A remote code execution vulnerability exists in Apache Struts as it does not properly handle requests containing the includeParams attribute. This could allow an attacker to execute arbitrary OGNL code on the victim's machine via a specially crafted request.

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-2013-1966, CVE-2013-2115
Advisory	http://struts.apache.org/development/2.x/docs/s2-014.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 2 before 2.3.14.2
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later), v6.82 (build 003 and later).
Associated Rule	tln-106938
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

