

## 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 DefaultActionMapper Prefixes OGNL Code Execution Vulnerability.

**Issue:** Apache Struts does not validate OGNL expressions in parameters with prefixes of action:, redirect:, and redirectAction:. This could allow an attacker to execute arbitrary OGNL expressions or gain access to sensitive information.

**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.

<b>Issue Identifier</b>	CVE-2013-2251
<b>Advisory</b>	<a href="http://struts.apache.org/release/2.3.x/docs/s2-016.html">http://struts.apache.org/release/2.3.x/docs/s2-016.html</a>
<b>Risk Assessment</b>	Important Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to gain access to sensitive information or execute arbitrary code.
<b>Affected Products</b>	Apache Struts 2.0.0 through 2.3.15
<b>Corero Products</b>	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).
<b>Associated Rule</b>	tIn-025193
<b>Associated Rule Set</b>	This rule is automatically enabled in the "Recommended Server Protection" rule set.

\* previously called TopResponse

<https://support.corero.com> Corero Network Security, Inc.  
One Cabot Road, Hudson, MA 01749 +1 978.212.1500 • Fax +1 978.212.1600  
• USA • Japan • Asia Pacific • EMEA Copyright 2013. All Rights Reserved.