S2-049

Summary

A DoS attack is available for Spring secured actions

Who should read this	All Struts 2 developers and users
Impact of vulnerability	A DoS attack is available for Spring secured actions
Maximum security rating	Important
Recommendation	Upgrade to Struts 2.5.12 or Struts 2.3.33
Affected Software	Struts 2.3.7 - Struts 2.3.32, Struts 2.5 - Struts 2.5.10.1
Reporter	Yasser Zamani <yasser dot zamani at live dot com>
CVE Identifier	CVE-2017-9787

Problem

When using a Spring AOP functionality to secure Struts actions it is possible to perform a DoS attack even if user was not properly authenticated but an application mixed secured and not secured actions in one class.

Solution

Upgrade to Apache Struts version 2.5.12 or 2.3.33.

Backward compatibility

No backward incompatibility issues are expected.

Workaround

Please define the below constant in a `struts.xml` file:

```
<constant name="struts.additional.excludedPatterns" value=".\.accessDecisionManager\.." />
```