S2-039

Summary

Getter as action method leads to security bypass

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible manipulation of return result and bypassing validation
Maximum security rating	Moderate
Recommendation	Upgrade to Struts 2.3.29.
Affected Software	Struts 2.3.20 - Struts Struts 2.3.28.1
Reporter	Takeshi Terada websec02 dot g02 at gmail.com
CVE Identifier	CVE-2016-4433

Problem

It is possible to pass a crafted request which can be used to bypass internal security mechanism and manipulate return string which can leads to redirecting user to unvalidated location.

Solution

Upgrade to Apache Struts version 2.3.29.

Backward compatibility

Some backward incompatibility issues are expected when upgrading to Struts 2.3.29 - it can happen that some OGNL expressions stop working because of performing disallowed arithmetic operations and assignments.

Workaround

You can try to use more restrictive RegEx used to clean up action names as below:

```
<constant name="struts.allowed.action.names" value="[a-zA-Z]*" />
```

Please adjust the RegEx to your action naming pattern, it should be as narrowed as possible.