S2-024

Summary

Wrong `excludeParams` overrides those defined in `DefaultExcludedPatternsChecker`

Who should read this	All Struts 2 developers and users
Impact of vulnerability	If default settings are used, the attacker can compromise internal state of an application
Maximum security rating	Moderate
Recommendation	Developers should immediately upgrade to Struts 2.3.20.1 or introduce the below change in framework's settings
Affected Software	Struts 2.3.20
Reporter	Jasper Rosenberg at Cargurus
CVE Identifier	CVE-2015-1831

Problem

Wrong default exclude patterns were introduced in version 2.3.20 of Struts, if default settings are used, the attacker can compromise internal application's state.

Solution

In Struts 2.3.20.1 a better set of exlude patterns was defined.

Backward compatibility

No backward compatibility problems are expected.

Workaround

If you cannot migrate to the latest version it's highly recommended to re-define `defaultStack` from `struts-default.xml` to this one below (or any other which is used in your application and drop `excludeParams` parameter):

Redefined defaultStack

```
<interceptor-stack name="myDefaultStack">
    <interceptor-ref name="exception"/>
    <interceptor-ref name="alias"/>
    <interceptor-ref name="servletConfig"/>
    <interceptor-ref name="i18n"/>
    <interceptor-ref name="prepare"/>
    <interceptor-ref name="chain"/>
    <interceptor-ref name="scopedModelDriven"/>
    <interceptor-ref name="modelDriven"/>
    <interceptor-ref name="fileUpload"/>
    <interceptor-ref name="checkbox"/>
    <interceptor-ref name="datetime"/>
    <interceptor-ref name="multiselect"/>
    <interceptor-ref name="staticParams"/>
    <interceptor-ref name="actionMappingParams"/>
    <interceptor-ref name="params"/>
    <interceptor-ref name="conversionError"/>
    <interceptor-ref name="validation">
        <param name="excludeMethods">input,back,cancel,browse</param>
    </interceptor-ref>
    <interceptor-ref name="workflow">
        <param name="excludeMethods">input,back,cancel,browse</param>
    </interceptor-ref>
    <interceptor-ref name="debugging"/>
    <interceptor-ref name="deprecation"/>
</interceptor-stack>
```

and define the following constant in `struts.xml`

```
<constant name="struts.additional.excludedPatterns" value="^(action|method):.*"/>
```