S2-057

Summary

Possible Remote Code Execution when `alwaysSelectFullNamespace` is `true` (either by user or a plugin like Convention Plugin) and then: results are used with no `namespace` and in same time, its upper `package` have no or wildcard `namespace` and similar to results, same possibility when using `url` tag which doesn't have `value` and `action` set and in same time, its upper `package` have no or wildcard `namespace`.

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible Remote Code Execution when `alwaysSelectFullNamespace` is `true` (either by user or a plugin like Convention Plugin) and then: results are used with no `namespace` and in same time, its upper `package` have no or wildcard `namespace` and similar to results, same possibility when using `url` tag which doesn't have `value` and `action` set and in same time, its upper `package` have no or wildcard `namespace`.
Maximum security rating	Critical
Recommendation	Upgrade to Struts 2.3.35 or Struts 2.5.17
Affected Software	Struts 2.0.4 - Struts 2.3.34, Struts 2.5.0 - Struts 2.5.16
Reporter	Man Yue Mo from the Semmle Security Research team
CVE Identifier	CVE-2018-11776

Problem

It is possible to perform a RCE attack when `alwaysSelectFullNamespace` is `true` (either by user or a plugin like Convention Plugin) and then: `namespace` value isn't set for a result defined in underlying configurations and in same time, its upper `package` configuration have no or wildcard `namespace` and same possibility when using `url` tag which doesn't have `value` and `action` set and in same time, its upper `package` configuration have no or wildcard `namespace`.

Solution

Upgrade to Apache Struts version 2.3.35 or 2.5.17.

Backward compatibility

Both 2.3.35 and 2.5.17 versions contain the security fixes only, nothing more. No backward incompatibility issues are expected.

We do get reports that in some cases backward compatibility issues can occur, it is related to usage of `ArrayList` directly in conversion logic. You should see a WARN in logs that the `ArrayList` is excluded. In such case please define the below constant in your `struts.xml`

```
<constant name="struts.excludedPackageNames" value="
    ognl.,
    javax.,
    freemarker.core.,
    freemarker.template.,
    freemarker.ext.rhino.,
    sun.reflect.,
    javassist.,
    com.opensymphony.xwork2.ognl.,
    com.opensymphony.xwork2.security."
/>
```

We are working on a new release to fix that problem.

Workaround

This is a temporal weak workaround. Please upgrade to Apache Struts version 2.3.35 or 2.5.17 ASAP because they also contain critical overall proactive security improvements

Verify that you have set (and always not forgot to set) `namespace` for all defined `packages`. Or verify that you have set (and always not forgot to set) `namespace` for all defined results (if it is applicable) and verify that you have set (and always not forgot to set) `value` or `action` for all `url` tags in your JSPs, when their upper `package` have no or wildcard `namespace`.

Struts 1

As we do not perform any tests against Struts 1 (Struts 1 was announced EOL) we cannot confirm that this version of Struts is not affected by the vulnerability. An example PoC was using an OGNL expression to perform RCE attack, so you can assume Struts 1 is safe as it doesn't base on OGNL.