S2-053

Summary

A possible Remote Code Execution attack when using an unintentional expression in Freemarker tag instead of string literals

Who should read this	All Struts 2 developers and users
Impact of vulnerability	A RCE attack is possible when developer is using wrong construction in Freemarker tags
Maximum security rating	Moderate
Recommendation	Upgrade to Struts 2.5.12 or Struts 2.3.34
Affected Software	Struts 2.0.0 - 2.3.33 Struts 2.5 - Struts 2.5.10.1
Reporter	Lupin <lupin1314 at gmail dot com> - jd.com security team David Greene <david at trumpetx dot com> Roland McIntosh <struts at rgm dot nu>
CVE Identifier	CVE-2017-12611

Problem

When using expression literals or forcing expression in Freemarker tags (see example below) and using request values can lead to RCE attack.

```
<@s.hidden name="redirectUri" value=redirectUri />
<@s.hidden name="redirectUri" value="${redirectUri}" />
<@s.hidden name="${redirectUri}"/>
```

In both cases a writable property is used in the `value` attribute and in both cases this is threatened as an expression by Freemarker. Please be aware that using Struts expression evaluation style is safe:

```
<@s.hidden name="redirectUri" value="%{redirectUri}" />
<@s.hidden name="%{redirectUri}"/>
```

Solution

Do not use such constructions in your code or use read-only properties to initialise the `value` attribute (property with getter only). You can upgrade to Apache Struts version 2.5.12 or 2.3.34 which contain more restricted Freemarker configuration but removing vulnerable constructions is preferable.

Backward compatibility

No backward incompatibility issues are expected.

Workaround

Inspect your code and remove vulnerable constructions.