S2-048

Summary

Possible RCE in the Struts Showcase app in the Struts 1 plugin example in Struts 2.3.x series

Who should read this	All Struts 2 developers and users should read this
Impact of vulnerability	Possible RCE when using the Struts 2 Struts 1 plugin
Maximum security rating	High
Recommendation	Please read the Solution section
Affected Software	Struts 2.3.x with Struts 1 plugin and Struts 1 action
Reporter	icez <ic3z at qq dot com> from Tophant Competence Center
CVE Identifier	CVE-2017-9791

Problem

It is possible to perform a RCE attack with a malicious field value when using the Struts 2 Struts 1 plugin and it's a Struts 1 action and the value is a part of a message presented to the user, i.e. when using untrusted input as a part of the error message in the `ActionMessage` class.

Solution

Always use resource keys instead of passing a raw message to the `ActionMessage` as shown below, never pass a raw value directly

```
messages.add("msg", new ActionMessage("struts1.gangsterAdded", gform.getName()));
```

and never like this

```
messages.add("msg", new ActionMessage("Gangster " + gform.getName() + " was added"));
```

Backward compatibility

No backward incompatibility issues are expected.