S2-030

Summary

Possible XSS vulnerability in `I18NInterceptor`

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible XSS vulnerability
Maximum security rating	Low
Recommendation	Do not expose parts of `Locale` object constructed by `I18NInterceptor` as it may contain user specific string which may leads to XSS vulnerability. Alternatively upgrade to Struts 2.3.28.
Affected Software	Struts 2.0.0 - Struts Struts 2.3.24.1
Reporter	Paolo Perliti paolo dot perliti at miliaris dot it - Miliaris
CVE Identifier	CVE-2016-2162

Problem

The Apache Struts framework uses `I18NInterceptor` to allow users and developers switch language used in the framework and an application built on top of it. The problem is that the interceptor doesn't perform any validation of the user input and accept arbitrary string which can be used by a developer to display language selected by the user. However, the framework doesn't expose the value directly in UI.

Solution

If you want present language selected by user based on `I18NInterceptor` always escape the string before presenting it to the user. Alternatively upgrad e to Struts 2.3.28.

Backward compatibility

No issues expected when upgrading to Struts 2.3.28.

Workaround

When needed you can use StringEscapeUtils from the Apache Commons to escape the string.