S2-027

Summary

`TextParseUtil.translateVariables` does not filter malicious OGNL expressions

Who should read this	All Struts 2 developers
Impact of vulnerability	Remote Code Execution, when unsanitized user input is passed to the method by a developer
Maximum security rating	Low
Recommendation	Don't pass unsanitized input to the said method or ActionSupport's getText methods. An upgrade to Struts 2.3.24.1 is recommended.
Affected Software	Struts 2.0.0 - Struts Struts 2.3.16.3
Reporter	Huawei PSIRT Team
CVE Identifier	CVE-2016-3090

Problem

`TextParseUtil.translateVariables` evaluates a given String with OGNL. Before Struts 2.3.20, a specially crafted String incorporating ANTLR tooling can, when passed to said method, cause a remote code execution.

The Struts 2 framework does not pass any user modifiable input to this method, neither directly nor indirectly. However, a developer crafting a Struts based web application might pass unsanitized user input to TextParseUtil.translateVariables or ActionSupport's getText methods. In that case a RCE exploitation might be possible.

Solution

- don't pass unsanitized user input to framework methods that include OGNL expression evaluation
- upgrade to Struts 2.3.24.1. Since Struts 2.3.20 advanced filtering was applied to this and similar methods involving OGNL evaluation.