S2-055

Summary

A RCE vulnerability in the Jackson JSON library

Who should read this	All Struts 2 developers and users which are using the REST plugin
Impact of vulnerability	It is possible perform a RCE attack using a crafted JSON payload, please read the linked issue for more details https://github.com/FasterXML/jackson-databind/issues/1599
Maximum security rating	High
Recommendation	Upgrade to Struts 2.5.14.1
Affected Software	Struts 2.5 - Struts 2.5.14
Reporter	David Dillard < david dot dillard at veritas dot com> - Veritas Technologies Product Security Group
CVE Identifier	Related to CVE-2017-7525

Problem

A RCE vulnerability was detected in the latest Jackson JSON library, which was reported here. Upgrade `com.fasterxml.jackson` to version 2.9.2 to address CVE-2017-7525.

Solution

Upgrade to Apache Struts version 2.5.14.1. Another solution is to manually upgrade Jackson dependencies in your project to not vulnerable versions, see this comment.

Backward compatibility

No backward incompatibility issues are expected.

Workaround

Upgrade Jackson JSON library to the latest version.