S2-051

Summary

A remote attacker may create a DoS attack by sending crafted xml request when using the Struts REST plugin

Who should read this	All Struts 2 developers and users
Impact of vulnerability	A DoS attack is possible when using outdated XStream library with the Struts REST plugin
Maximum security rating	Medium
Recommendation	Upgrade to Struts 2.5.13 or Struts 2.3.34
Affected Software	Struts 2.1.6 - 2.3.33 Struts 2.5 - 2.5.12
Reporter	Huijun Chen, Xiaolong Zhu
CVE Identifier	CVE-2017-9793

Problem

The REST Plugin is using outdated XStream library which is vulnerable and allow perform a DoS attack using malicious request with specially crafted XML payload.

Solution

Upgrade to Apache Struts version 2.5.13 or 2.3.34.

Backward compatibility

No backward incompatibility issues are expected.

Workaround

When using Maven, you can exclude the XStream library and use the latest 1.4.10 version. In other case replace the XStream jar in your final distribution package.