S2-035

Summary

Action name clean up is error prone

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible way to craft vulnerable payload
Maximum security rating	Low
Recommendation	Upgrade to latest version of the Apache Struts, 2.3.29 or 2.5.1.
Affected Software	Struts 2.0.0 - Struts 2.3.28.1
Reporters	Alvaro Munoz alvaro dot munoz at hpe dot com Sam Ng samn at hpe dot com
CVE Identifier	CVE-2016-4436

Problem

The method used to clean up action name can produce vulnerable payload based on crafted input which can be used by attacker to perform unspecified attack.

Solution

You should upgrade to latest Struts version or implement your own version of `ActionMapper` based on source code of receomened Struts versions.

Backward compatibility

No issues expected when upgrading Struts version.

Workaround

Implement your own version of clean up method which will throw an exception.