S2-018

Summary

Broken Access Control Vulnerability in Apache Struts2

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Permissions, Privileges, and Access Controls
Maximum security rating	Important
Recommendation	Developers should immediately upgrade to Struts 2.3.15.3
Affected Software	Struts 2.0.0 - Struts 2.3.15.2
Reporter	Zhu Gang, Zhang Jin, Huawei PSIRT
CVE Identifier	CVE-2013-4310

Problem

The Struts 2 action mapping mechanism supports the special parameter prefix action: which is intended to help with attaching navigational information to buttons within forms.

In Struts 2 before 2.3.15.3, under certain conditions this can be used to bypass security constraints. More details will available later on when the patch will be widely adopted.

Solution

In Struts 2.3.15.3 the action mapping mechanism was changed to avoid circumventing security constraints. Two additional constants were introduced to steer behaviour of DefaultActionMapper:

- struts.mapper.action.prefix.enabled - when set to false support for "action:" prefix is disabled, set to false by default
- struts.mapper.action.prefix.crossNamespaces - when set to false, actions defined with "action:" prefix must be in the same namespace as current action

Backward Compatibility

After upgrading to Struts 2.3.15.3, applications using the "action:" will stop working. You can use above constants to steer that behaviour.

It is strongly recommended to upgrade to Struts 2.3.15.3, which contains the corrected Struts2-Core library.