S2-032

Summary

Remote Code Execution can be performed via `method:` prefix when Dynamic Method Invocation is enabled.

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible Remote Code Execution
Maximum security rating	High
Recommendation	Disable Dynamic Method Invocation if possible. Alternatively upgrade to Struts 2.3.20.3, Struts 2.3.24.3 or Struts 2.3.28.1.
Affected Software	Struts 2.3.20 - Struts Struts 2.3.28 (except 2.3.20.3 and 2.3.24.3)
Reporter	Nike Zheng nike dot zheng at dbappsecurity dot com dot cn
CVE Identifier	CVE-2016-3081

Problem

It is possible to pass a malicious expression which can be used to execute arbitrary code on server side when Dynamic Method Invocation is enabled.

Solution

Disable Dynamic Method Invocation when possible or upgrade to Apache Struts versions 2.3.20.3, 2.3.24.3 or 2.3.28.1.

Backward compatibility

No issues expected when upgrading to Struts 2.3.20.3, 2.3.24.3 and 2.3.28.1

Workaround

Disable Dynamic Method Invocation or implement your own version of `ActionMapper` based on a source code of the recommended Apache Struts versions.