S2-034

Summary

OGNL cache poisoning can lead to DoS vulnerability

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible DoS attack
Maximum security rating	Important
Recommendation	This issue was resolved by publising new OGNL version, any Struts version which at least is using OGNL 3.0.12 is safe.
Affected Software	Struts 2.0.0 - Struts 2.3.24.1
Reporters	Tao Wang wangtao12 at baidu dot com - Baidu Security Response Center
CVE Identifier	CVE-2016-3093

Problem

The OGNL expression language used by the Apache Struts framework has inproper implementaion of cache used to store method references. It's possible to prepare a DoS attack which can block access to a web site.

Solution

You can should upgrade OGNL at least to version 3.0.12 or by upgrading to latest Struts version.

Backward compatibility

No issues expected when upgrading to OGNL or Struts.

Workaround

Not possible except upgrading OGNL as mentioned above.