S2-021

Summary

Improves excluded params in ParametersInterceptor and CookieInterceptor to avoid ClassLoader manipulation

Who should read this	All Struts 2 developers and users
Impact of vulnerability	ClassLoader manipulation
Maximum security rating	High
Recommendation	Developers should immediately upgrade to Struts 2.3.16.2
Affected Software	Struts 2.0.0 - Struts 2.3.16.1
Reporter	NTT-CERT via JPCERT/CC, Takeshi Terada (Mitsui Bussan Secure Directions, Inc.), Takayoshi Isayama (Mitsui Bussan Secure Directions, Inc.), Yoshiyuki Karezaki (Yoshiyuki.Karezaki at scsk.jp) BAKA/ty (121605589 at qq.com), Nebula (Chibi, Hubei, CN), HelloWorld security team, NSFOCUS Security Team, heige (zhoujp at knownsec.com)
CVE Identifier	CVE-2014-0112 - Incomplete fix for ClassLoader manipulation via ParametersInterceptor CVE-2014-0113 - ClassLoader manipulation via CookieInterceptor when configured to accept all cookies

Problem

The excluded parameter pattern introduced in version 2.3.16.1 to block access to getClass() method wasn't sufficient. It is possible to omit that with specially crafted requests. Also CookieInterceptor is vulnerable for the same kind of attack when it was configured to accept all cookies (when "*" is used to configure `cookiesName` param).

Solution

In Struts 2.3.16.2 improved "class" pattern was introduced directly to ParametersInterceptor and CookieInterceptor.

Backward compatibility

No backward compatibility problems are expected.

Workaround

If you cannot upgrade to version 2.3.16.2 immediately - which is strongly advised - you can apply below workarounds:

Exclude 'class' parameter

Replace the previous class related pattern with '(.*\.|^|.*|\[('|"))class(\.|('|"))]|\[).*' on the list of excludeParams as below

```
<interceptor-ref name="params">
  <param name="excludeParams">(.*\.|^|.*|\[('|"))(c|C)lass(\.|('|")]|\[).*,
^dojo\..*,^struts\..*,^session\..*,^request\..*,^application\..*,^servlet
(Request|Response)\..*,^parameters\..*,^action:.*,^method:.*</param>
</interceptor-ref>
```

It isn't possible to do the same with CookieInterceptor, so don't use wildcard mapping to accept cookie names or implement your own version of CookieInterceptor based on code provided in Struts 2.3.16.2.

Please be aware that this workaround is not as complete as the corrections in Struts 2.3.16.2