S2-020

Summary

Upgrade Commons FileUpload to version 1.3.1 (avoids DoS attacks) and adds 'class' to exclude params in ParametersInterceptor (avoid ClassLoader manipulation)

Who should read this	All Struts 2 developers and users
Impact of vulnerability	DoS attacks and ClassLoader manipulation
Maximum security rating	Important
Recommendation	Developers should immediately upgrade to Struts 2.3.16.2
Affected Software	Struts 2.0.0 - Struts 2.3.16.1
Reporter	Peter Magnusson (peter.magnusson at omegapoint.se), Przemysaw Celej (p-celej at o2.pl)
CVE Identifier	CVE-2014-0050 (DoS), CVE-2014-0094 (ClassLoader manipulation)

Problem

The default upload mechanism in Apache Struts 2 is based on Commons FileUpload version 1.3 which is vulnerable and allows DoS attacks. Additional ParametersInterceptor allows access to 'class' parameter which is directly mapped to getClass() method and allows ClassLoader manipulation.

Solution

In Struts 2.3.16.1, Commons FileUpload was updated to version 1.3.1 and "class" was added to excludeParams in struts-default.xml configuration of ParametersInterceptor.

Backward compatibility

No backward compatibility problems are expected.

Workaround

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

Upgrade commons-fileupload

The fixed commons-fileupload library is a drop-in replacement for the vulnerable version. Deployed applications can be hardened by replacing the common s-fileupload jar file in WEB-INF/lib with the updated jar. For Maven
based Struts 2 projects, the following dependency needs to be added:

```
<dependency>
    <groupId>commons-fileupload</groupId>
    <artifactId>commons-fileupload</artifactId>
    <version>1.3.1</version>
</dependency>
```

Exclude 'class' parameter

Simple add '^class\.*' to the list of excludeParams as below

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