S2-029

Summary

Forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution.

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible Remote Code Execution vulnerability
Maximum security rating	Important
Recommendation	Always validate incoming parameters' values when re-assigning them to certain Struts' tags attributes. Don't use %{...} syntax in tag attributes other than *value* unless you have a valid use-case. Alternatively upgrade to Struts 2.3.20.3, Struts 2.3.24.3 or Struts 2.3.28
Affected Software	Struts 2.0.0 - Struts 2.3.24.1 (except 2.3.20.3)
Reporters	Romain Gaucher rgaucher at coverity dot com - Coverity Lupin lupin1314 at gmail dot com - jd.com security team nike.zheng at dbappsecurity dot com dot cn - dbappsecurity team genxors at gmail dot com - Qihoo 360 SkyEye Lab
CVE Identifier	CVE-2016-0785

Problem

The Apache Struts frameworks when forced, performs double evaluation of attributes' values assigned to certain tags so it is possible to pass in a value that will be evaluated again when a tag's attributes will be rendered.

Solution

Adding a proper validation of each value that's coming in and it's used in tag's attributes.

Don't use forced evaluation of an attribute other than *value* using %{...} syntax unless really needed for a valid use-case.

By upgrading to Struts 2.3.20.3, 2.3.24.3 and 2.3.28, possible malicious effects of forced double evaluation are limited.

Backward compatibility

No issues expected when upgrading to Struts 2.3.20.3, 2.3.24.3 and 2.3.28

Workaround

If you are using Struts 2.3.20, 2.3.24 or 2.3.24.1 you can redefine `struts.excludedClasses` as showed below, for more details please read internal security page.

```
    <constant name="struts.excludedClasses"
              value="
                java.lang.Object,
                java.lang.Runtime,
                java.lang.System,
                java.lang.Class,
                java.lang.ClassLoader,
                java.lang.Shutdown,
                java.lang.ProcessBuilder,
                ognl.OgnlContext,
                ognl.ClassResolver,
                ognl.TypeConverter,
                com.opensymphony.xwork2.ognl.SecurityMemberAccess,
                com.opensymphony.xwork2.ActionContext" />
```