S2-045

Summary

Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser.

Who should read this	All Struts 2 developers and users
Impact of vulnerability	Possible RCE when performing file upload based on Jakarta Multipart parser
Maximum security rating	Critical
Recommendation	Upgrade to Struts 2.3.32 or Struts 2.5.10.1
Affected Software	Struts 2.3.5 - Struts 2.3.31, Struts 2.5 - Struts 2.5.10
Reporter	Nike Zheng <nike dot zheng at dbappsecurity dot com dot cn>
CVE Identifier	CVE-2017-5638

Problem

It is possible to perform a RCE attack with a malicious `Content-Type` value. If the `Content-Type` value isn't valid an exception is thrown which is then used to display an error message to a user.

Solution

If you are using Jakarta based file upload Multipart parser, upgrade to Apache Struts version 2.3.32 or 2.5.10.1. You can also switch to a different implementation of the Multipart parser.

Backward compatibility

No backward incompatibility issues are expected.

Workaround

Implement a Servlet filter which will validate `Content-Type` and throw away request with suspicious values not matching `multipart/form-data`.

Other option is to remove the File Upload Interceptor from the stack, just define your own custom stack and set it as a default - please read How do we configure an Interceptor to be used with every Action. This will work only for Struts 2.5.8 - 2.5.10.

```
<interceptors>
    <interceptor-stack name="defaultWithoutUpload">
        <interceptor-ref name="exception"/>
        <interceptor-ref name="alias"/>
        <interceptor-ref name="servletConfig"/>
        <interceptor-ref name="i18n"/>
        <interceptor-ref name="prepare"/>
        <interceptor-ref name="chain"/>
        <interceptor-ref name="scopedModelDriven"/>
        <interceptor-ref name="modelDriven"/>
        <interceptor-ref name="checkbox"/>
        <interceptor-ref name="datetime"/>
        <interceptor-ref name="multiselect"/>
        <interceptor-ref name="staticParams"/>
        <interceptor-ref name="actionMappingParams"/>
        <interceptor-ref name="params"/>
        <interceptor-ref name="conversionError"/>
        <interceptor-ref name="validation">
            <param name="excludeMethods">input,back,cancel,browse</param>
        </interceptor-ref>
        <interceptor-ref name="workflow">
            <param name="excludeMethods">input,back,cancel,browse</param>
        </interceptor-ref>
        <interceptor-ref name="debugging"/>
    </interceptor-stack>
</interceptors>
<default-interceptor-ref name="defaultWithoutUpload"/>
```