

# S2-046

## Summary

Possible RCE when performing file upload based on Jakarta Multipart parser (similar to S2-045)

<b>Who should read this</b>	All Struts 2 developers and users
<b>Impact of vulnerability</b>	Possible RCE when performing file upload based on Jakarta Multipart parser
<b>Maximum security rating</b>	Critical
<b>Recommendation</b>	Upgrade to <a href="#">Struts 2.3.32</a> or <a href="#">Struts 2.5.10.1</a>
<b>Affected Software</b>	Struts 2.3.5 - Struts 2.3.31, Struts 2.5 - Struts 2.5.10
<b>Reporter</b>	Chris Frohoff <cfrohoff at qualcomm dot com>, Nike Zheng <nike dot zheng at dbappsecurity dot com dot cn>, Alvaro Munoz <alvaro dot munoz at hpe dot com>
<b>CVE Identifier</b>	CVE-2017-5638

## Problem

It is possible to perform a RCE attack with a malicious `Content-Disposition` value or with improper `Content-Length` header. If the `Content-Disposition/Content-Length` value is not valid an exception is thrown which is then used to display an error message to a user. This is a different vector for the same vulnerability described in S2-045 (CVE-2017-5638).

## Solution

If you are using Jakarta based file upload Multipart parser, upgrade to Apache Struts version 2.3.32 or 2.5.10.1.

## Backward compatibility

No backward incompatibility issues are expected.

## Workaround

You can switch to a different [implementation](#) of the Multipart parser. We have already prepared two plugins which can be used as a drop-in solution, please find them [here](#). You can use them when you are running the Apache Struts 2.3.8 - 2.5.5 (in case of using the default Jakarta multipart parser) or the Apache Struts 2.3.20 - 2.5.5 (when using an alternative [jakarta-stream](#) multipart parser).

Another 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"/>
```