1759134370 / iot Public

Code Issues Pull requests Actions Projects Wiki Security ...

main

iot / TOTOLINK / A860R / 6.md

1759134370 Create 6.md History

1 contributor

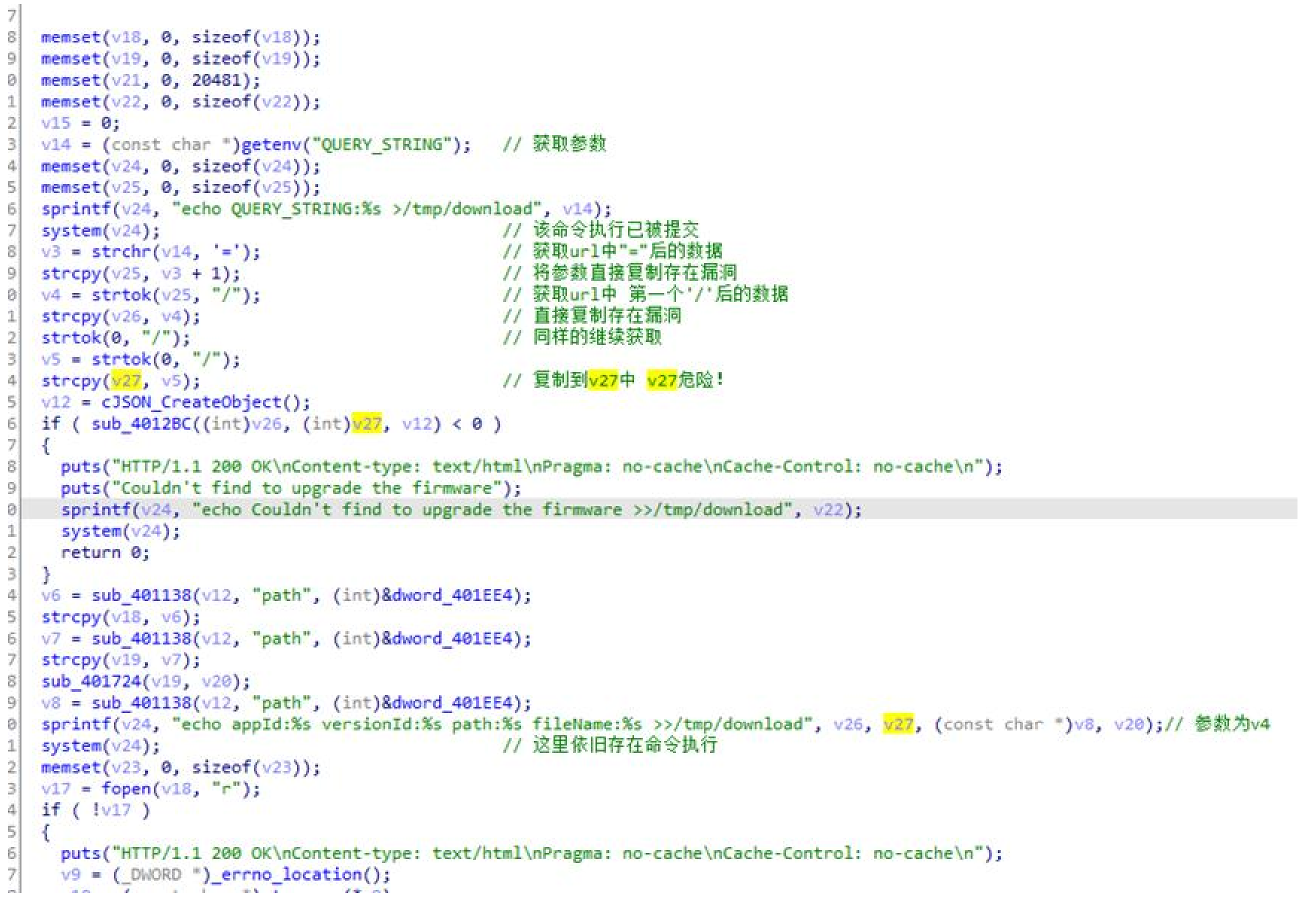
19 lines (10 sloc) | 640 Bytes

Firmware:

TOTOLINK:A860R V4.1.2cu.5182_B20201027

http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=62&ids=36

Detail:



```
memset(v18, 0, sizeof(v18));
memset(v19, 0, sizeof(v19));
memset(v21, 0, 20481);
memset(v22, 0, sizeof(v22));
v15 = 0;
v14 = (const char *)getenv("QUERY_STRING");   // 获取参数
memset(v24, 0, sizeof(v24));
memset(v25, 0, sizeof(v25));
sprintf(v24, "echo QUERY_STRING:%s >/tmp/download", v14);
system(v24);                                  // 该命令执行已被提交
v3 = strchr(v14, '=');                        // 获取url中"="后的数据
strcpy(v25, v3 + 1);                          // 将参数直接复制存在漏洞
v4 = strtok(v25, "/");                        // 获取url中 第一个'/'后的数据
strcpy(v26, v4);                              // 直接复制存在漏洞
strtok(0, "/");                               // 同样的继续获取
v5 = strtok(0, "/");
strcpy(v27, v5);                              // 复制到v27中 v27危险!
v12 = cJSON_CreateObject();
if ( sub_4012BC((int)v26, (int)v27, v12) < 0 )
{
  puts("HTTP/1.1 200 OK\nContent-type: text/html\nPragma: no-cache\nCache-Control: no-cache\n");
  puts("Couldn't find to upgrade the firmware");
  sprintf(v24, "echo Couldn't find to upgrade the firmware >>/tmp/download", v22);
  system(v24);
  return 0;
}
v6 = sub_401138(v12, "path", (int)&dword_401EE4);
strcpy(v18, v6);
v7 = sub_401138(v12, "path", (int)&dword_401EE4);
strcpy(v19, v7);
sub_401724(v19, v20);
v8 = sub_401138(v12, "path", (int)&dword_401EE4);
sprintf(v24, "echo appId:%s versionId:%s path:%s fileName:%s >>/tmp/download", v26, v27, (const char *)v8, v20);// 参数为v4
system(v24);                                  // 这里依旧存在命令执行
memset(v23, 0, sizeof(v23));
v17 = fopen(v18, "r");
if ( !v17 )
{
  puts("HTTP/1.1 200 OK\nContent-type: text/html\nPragma: no-cache\nCache-Control: no-cache\n");
  v9 = (_DWORD *)_errno_location();
```

V14 Obtains the data transferred by the front end through GET

Then the program copied the data into V27 after splitting the "/" data several times .

Then through

Sprintf (v24, "echo appId:%s versionId:%s path:%s fileName:%s >>/ TMP /download", V26, v27, (const char *) V8, V20);

This line of functions copies the data into the V24 array, and again executes directly with System