TP-Link M7350 V3 190531存在未认证命令注入漏洞

漏洞说明

漏洞：固件命令注入漏洞

影响固件：TP-Link M7350 V3

影响版本：V3 190531

此漏洞是因为参数没有过滤导致可以通过拼接绕过直接执行命令。

不同于 CVE-2019-12104 <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12104> 和CVE-2019-12103 <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12103> （ CNVD-2019-31312和CNVD-2019-31307），在版本TP-LINK M7350 V3 190531都修复了这两个漏洞，而这个漏洞则是针对TP-LINK M7350 V3 190531版本的固件的漏洞。

漏洞原理

漏洞针对的TP-LINK M7350 V3 190531可以在链接中获取，

qcmap_web_cgi文件处理web请求并接收参数，在FUN_000092ec函数中，将参数推送到qcmap_webclient_cgi_file。

```
31    g_strlcat(s[0].sa_data, "/www/qcmap_cgi_webclient_file", 108);
32    unlink(s[0].sa_data);
33    v10 = strlen(s[0].sa_data);
34    if ( bind(*a5, s, v10 + 2) == -1 )
35    {
36      close(*a5);
37      *a4 = 30;
38      g_strlcat(a3, "{\"commit\":\"Socket Bind Error\"}", 40960);
39      result = -1;
40    }
41    else
42    {
43      addr.sa_family = 1;
44      g_strlcat(addr.sa_data, "/www/qcmap_webclient_cgi_file", 108);
45      system("chmod 777 /www/qcmap_cgi_webclient_file");
46      v11 = strlen(addr.sa_data);
47      v12 = sendto(*a5, a1, a2, 0, &addr, v11 + 2);
48      if ( v12 == -1 )
49      {
50        close(*a5);
```

然后QCMAP_Web_CLIENT文件接受并读取参数，在偏移为0x15384处的代码块读取language参数，并直接使用snprintf拼接，然后放入popen函数执行命令，此处可以控制参数language的内容进行命令注入。如下图

```
37    case 1:
38      v14 = cJSON_GetObjectItem(a1, "language");
39      v15 = v14;
40      if ( !v14 )
41        goto LABEL_10;
42      v16 = *(const char **)(v14 + 16);
43      if ( !v16 )
44        goto LABEL_10;
45      snprintf(s, 0xC8u, "uci set webserver.user_config.language='%s';uci commit webserver", v16);
46      if ( !sub_14A1C(s) )
47        goto LABEL_10;
48      v5 = 0;
49      snprintf(
50        s,
```

漏洞复现

因为命令无法回显，所以使用打开telnet的命令。

Poc：

```
:~$ telnet 192.168
Trying 192.168.  ...
telnet: Unable to connect to remote host: Connection refused
:~$ telnet 192.168.
Trying 192.168.  ...
Connected to 192.168.
Escape character is '^]'.
```

修复建议

对参数过滤引号

参考链接

https://www.tp-link.com/uk/support/download/m7350/v3/#Firmware <https://www.tp-link.com/uk/support/download/m7350/v3/#Firmware>