TRCwifiZone Hotspot Authentication Bypass

2020.08.10

M. Haluk Kuscuoglu (https://cxsecurity.com/author/M.+Haluk+Kuscuoglu/1/) (TR)

Risk: Medium | Local: Yes | Remote: Yes

CVE: N/A | CWE: N/A

```
# Exploit Title: TRCwifiZone Authentication Bypass
# Date: 08.09.2020
# Exploit Author: M. Haluk Kuscuoglu
# Vendor: Turcom
# Software Link: https://www.turcom.com.tr/urunlerimiz-sorunsuz-internet-trcwifizone.asp
# Version: All
# Tested on: Windows 10
# CVE: -


Description: TRCwifiZone is the hotspot solution of Turcom company.

Vulnerability Point: http://trcwifizone/manage/

Trigger Example: http://trcwifizone/manage/control.php

Exploitation Method: Call admin panel link http://trcwifizone/manage/control.php while your proxy tool (reccomended Burp Suite) enabled.
Then, look 302 redirection response and you will see admin panel page.

PoC Screenshots:

1. https://imgur.com/xt9FHkL
2. https://imgur.com/jHY6kpA
3. https://imgur.com/bKsWgy4
4. https://imgur.com/7cHev8j
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020080046)

Tr | Lul

Vote for this issue: 1 0

100%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)