



# CVE-2022-29394

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2022-29394   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2022-05-10 20:15:00 UTC  |
| <b>Updated</b>         | 2022-05-16 17:18:00 UTC  |
| <b>Description</b>     | TOTOLINK N600R V4.3.0cu.7647_B20210106 was discovered to contain a stack overflow via the macAddress parameter i |

## Risk And Classification

**Problem Types: CWE-787**

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                   | Product        | Version                | Update | Edition | Language |
|------------------|--------------------------|----------------|------------------------|--------|---------|----------|
| Hardware         | <a href="#">Totolink</a> | N600r          | -                      | All    | All     | All      |
| Operating System | <a href="#">Totolink</a> | N600r Firmware | 4.3.0cu.7647_b20210106 | All    | All     | All      |

## References

| Reference   | Source  | Link                         | Tags                |
|---|---------|------------------------------|---------------------|
| IoT-vuln/Totolink/1.setWiFiAclAddConfig at main · d1tto/loT-vuln · GitHub | MISC    | <a href="#">github.com</a>   |                     |
| CVE Program record  | CVE.ORG | <a href="#">www.cve.org</a>  | canonical           |
| NVD vulnerability detail  | NVD     | <a href="#">nvd.nist.gov</a> | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**