



# CVE-2022-40109

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2022-40109  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2022-09-06 17:15:00 UTC   |
| <b>Updated</b>         | 2022-09-09 15:24:00 UTC   |
| <b>Description</b>     | TOTOLINK A3002R TOTOLINK-A3002R-He-V1.1.1-B20200824.0128 is vulnerable to Insecure Permissions via binary /bin/ |

## Risk And Classification

**Problem Types:** CWE-276

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor   | Product         | Version              | Update | Edition | Language |
|------------------|----------|-----------------|----------------------|--------|---------|----------|
| Hardware         | Totolink | A3002r          | -                    | All    | All     | All      |
| Operating System | Totolink | A3002r Firmware | 1.1.1-b20200824.0128 | All    | All     | All      |

## References

| Reference                                  | Source  | Link  | Tags                |
|--|---------|---|---------------------|
| iot/1.md at main · 1759134370/iot · GitHub | MISC    | <a href="https://github.com">github.com</a>     |                     |
| CVE Program record                         | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>   | canonical           |
| NVD vulnerability detail                   | NVD     | <a href="https://nvd.nist.gov">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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)