



# CVE-2026-31170

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

## Summary

<b>CVE</b>	CVE-2026-31170
<b>State</b>	PUBLISHED
<b>Assigner</b>	mitre
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-09 19:16:23 UTC
<b>Updated</b>	2026-04-09 19:16:23 UTC
<b>Description</b>	An issue was discovered in ToToLink A3300R firmware v17.0.0cu.557_B20221024 allowing attackers to execute arbitrary c

## Risk And Classification

**EPSS:** 0.000130000 probability, percentile 0.022240000 (date 2026-04-11)

**Problem Types:** n/a

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

## References

Reference	Source	Link	Tags
github.com/Svigo-o/TOTOLINK-Vul/tree/main/totolink-a3300r-stun-pass-cmd-...	cve@mitre.org	<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](#).

**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)