



# CVE-2023-41554

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2023-41554   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2023-08-30 13:15:00 UTC  |
| <b>Updated</b>         | 2023-08-31 18:40:00 UTC  |
| <b>Description</b>     | Tenda AC9 V3.0 V15.03.06.42_multi was discovered to contain a stack overflow via parameter wpapsk_crypto at url /gofor |

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                | Product                      | Version          | Update | Edition | Language |
|------------------|-----------------------|------------------------------|------------------|--------|---------|----------|
| Hardware         | <a href="#">Tenda</a> | <a href="#">Ac9</a>          | 3.0              | All    | All     | All      |
| Operating System | <a href="#">Tenda</a> | <a href="#">Ac9 Firmware</a> | 5.03.06.42_multi | All    | All     | All      |

## References

| Reference                | Source  | Link                         | Tags                |
|--------------------------|---------|------------------------------|---------------------|
| Affected Version         | 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](#).

**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)