



# CVE-2022-36053

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

## Summary

<b>CVE</b>	CVE-2022-36053
<b>State</b>	PUBLIC
<b>Assigner</b>	security-advisories@github.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-09-01 12:15:00 UTC
<b>Updated</b>	2022-09-07 15:31:00 UTC
<b>Description</b>	Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. The low-power IPv6 network

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Contiki-ng</a>	<a href="#">Contiki-ng</a>	All	All	All	All

## References

### Reference

- [Out-of-bounds read in the uIP buffer module · Advisory · contiki-ng/contiki-ng · GitHub](#)
- [uipbuf: Do not assume that there is enough space for a following extension header by nvt · Pull Request #1648 · contiki-ng/contiki-ng · GitHub](#)
- [CVE Program record](#)
- [NVD vulnerability detail](#)

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](#)**