# CVE-2020-25860

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-25860 |
| **State** | PUBLIC |
| **Assigner** | vuln@vdoo.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2020-12-21 18:15:00 UTC |
| **Updated** | 2020-12-29 14:36:00 UTC |
| **Description** | The install.c module in the Pengutronix RAUC update client prior to version 1.5 has a Time-of-Check Time-of-Use vulnerab |

## Risk And Classification

**Problem Types:** CWE-367

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Pengutronix | Rauc | All | All | All | All |
| Application | Pengutronix | Rauc | All | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| Time-of-Check-Time-of-Use Vulnerability · Advisory · rauc/rauc · GitHub | MISC | github.com | Explo |
| CVE-2020-25860 - Significant vulnerability discovered in RAUC embedded firmware update framework | MISC | www.vdoo.com | Explo |
| CVE Program record | CVE.ORG | www.cve.org | cano |
| NVD vulnerability detail | NVD | nvd.nist.gov | cano |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

180621 Debian Security Update for rauc (CVE-2020-25860)

**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status status.cve.report**