



# CVE-2020-25860

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

## Summary

<b>CVE</b>	CVE-2020-25860
<b>State</b>	PUBLIC
<b>Assigner</b>	vuln@vdoo.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-12-21 18:15:00 UTC
<b>Updated</b>	2020-12-29 14:36:00 UTC
<b>Description</b>	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	<a href="#">Pengutronix</a>	<a href="#">Rauc</a>	All	All	All	All
Application	<a href="#">Pengutronix</a>	<a href="#">Rauc</a>	All	All	All	All

## References

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

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)