CVE-2022-25051

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

Summary

CVE	CVE-2022-25051
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-02 00:15:00 UTC
Updated	2022-03-14 14:07:00 UTC
Description	An Off-by-one Error occurs in cmr113_decode of rtl_433 21.12 when decoding a crafted file.

Risk And Classification

Problem Types: CWE-193

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rtl 433 Project	Rtl 433	21.12	All	All	All

References

Reference	Source	Link
Responsible disclosure policy · Issue #1960 · merbanan/rtl_433 · GitHub	MISC	github.com
minor: Fix overflow in Clipsal-CMR113 and Somfy-IOHC reported by aug5t7 · merbanan/rtl_433@2dad7b9 · GitHub	MISC	github.com
huntr – the Bug Bounty Platform for any GitHub repository	MISC	huntr.dev
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184983 Debian Security Update for rtl-433 (CVE-2022-25051)

502950 Alpine Linux Security Update for rtl_433

505819 Alpine Linux Security Update for rtl_433

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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 registred 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