CVE-2022-38394

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

Summary

CVE	CVE-2022-38394
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-08 08:15:00 UTC
Updated	2022-09-13 15:09:00 UTC
Description	Use of hard-coded credentials for the telnet server of CentreCOM AR260S V2 firmware versions prior to Ver.3.3.7 allows a

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Allied-telesis	Centrecom Ar260s	v2	All	All	All
Operating System	Allied-telesis	Centrecom Ar260s Firmware	All	All	All	All

References

Reference	Source	Link	Tags
JVN#45473612: Multiple vulnerabilities in CentreCOM AR260S V2	MISC	jvn.jp	
www.allied-telesis.co.jp/support/list/faq/vuls/20220829.html	MISC	www.allied-telesis.co.jp	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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