CVE-2023-28725

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

Summary

CVE	CVE-2023-28725
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-22 00:15:00 UTC
Updated	2023-03-27 22:19:00 UTC
Description	General Bytes Crypto Application Server (CAS) 20230120, as distributed with General Bytes BATM devices, allows remote

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Generalbytes	Crypto Application Server	20230120	All	All	All

References

Reference	Source	Link	Tags
Security Incident March 17-18th 2023 - General Bytes Knowledge Base - Confluence	MISC	generalbytes.atlassian.net	
Update CAS - General Bytes Knowledge Base - Confluence	MISC	generalbytes.atlassian.net	
JavaScript is not available.	MISC	twitter.com	
General Bytes Bitcoin ATMs hacked using zero-day, $1.5M stolen	MISC	www.bleepingcomputer.com	
General Bytes crypto ATMs exploited for over $1.6 million	MISC	web3isgoinggreat.com	
Hackers drain bitcoin ATMs of $1.5 million by exploiting 0-day bug | Ars Technica	MISC	arstechnica.com	
Changelog | GENERAL BYTES	MISC	www.generalbytes.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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