CVE-2022-2582

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

Summary

CVE	CVE-2022-2582
State	PUBLIC
Assigner	security@golang.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-27 22:15:00 UTC
Updated	2023-01-05 04:43:00 UTC
Description	The AWS S3 Crypto SDK sends an unencrypted hash of the plaintext alongside the ciphertext as a metadata field. This has

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Amazon	Aws Software Development Kit	All	All	All	All

References

Reference	Source	Link	Tags
service/s3/s3crypto: V2 Client Release (#3403) · aws/aws-sdk-go@35fa6dd · GitHub	MISC	github.com	
GO-2022-0391 - Go Packages	MISC	pkg.go.dev	
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.

Legacy QID Mappings

181452 Debian Security Update for golang-github-aws-aws-sdk-go (CVE-2022-2582)

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