



CVE-2021-20327

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

Summary

CVE	CVE-2021-20327
State	PUBLIC
Assigner	cna@mongodb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-25 17:15:00 UTC
Updated	2021-03-04 20:38:00 UTC
Description	A specific version of the Node.js mongodb-client-encryption module does not perform correct validation of the KMS server's

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	MongoDB	Libmongocrypt	1.2.0	All	All	All
Application	MongoDB	Libmongocrypt	1.2.0	All	All	All

References

Reference	Source	Link	Tags
[NODE-3125] Node CSFLE Not Validating KMS Certificate - MongoDB	MISC	jira.mongodb.org	Vendor Advisory
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

983841 Nodejs (npm) Security Update for mongodb-client-encryption (GHSA-rjmf-p882-645m)

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](#).

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