



CVE-2021-34802

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

Summary

CVE	CVE-2021-34802
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-30 14:15:00 UTC
Updated	2021-08-04 00:52:00 UTC
Description	A failure in resetting the security context in some transaction actions in Neo4j Graph Database 4.2 and 4.3 could allow auth

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Neo4j	Graph Database	4.2	All	All	All
Application	Neo4j	Graph Database	4.3	All	All	All

References

Reference	Source	Link	Tags
Graph Data Platform Graph Database Management System Neo4j	MISC	neo4j.com	
Neo4j 4.2.x Security Vulnerability Fixed in Release 4.2.8 - Knowledge Base	MISC	neo4j.com	
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 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](#).

Free CVE JSON API cve.report/api

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