



CVE-2023-31136

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

Summary

CVE	CVE-2023-31136
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-09 14:15:00 UTC
Updated	2023-05-16 16:43:00 UTC
Description	PostgresNIO is a Swift client for PostgreSQL. Any user of PostgresNIO prior to version 1.14.2 connecting to servers with TL

Risk And Classification

Problem Types: CWE-522

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vapor	Postgresnio	All	All	All	All

References

Reference	S
When the server is configured to use trust authentication... · CVE-2021-23214 · GitHub Advisory Database · GitHub	M
PostgreSQL: CVE-2021-23214: Server processes unencrypted bytes from man-in-the-middle	M
A man-in-the-middle attacker can inject false responses... · CVE-2021-23222 · GitHub Advisory Database · GitHub	M
PostgresNIO processes unencrypted bytes from man-in-the-middle · Advisory · vapor/postgres-nio · GitHub	M
Release PostgresNIO 1.14.2 · vapor/postgres-nio · GitHub	M
PostgreSQL: CVE-2021-23222: libpq processes unencrypted bytes from man-in-the-middle	M
Merge pull request from GHSA-9cfh-vx93-84vv · vapor/postgres-nio@2df54bc · GitHub	M
Add unprocessedBytes property on NIOSingleStepByteToMessageProcessor by fabianfett · Pull Request #2419 · apple/swift-nio · GitHub	M
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#)