



CVE-2021-43767

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

Summary

CVE	CVE-2021-43767
State	PUBLIC
Assigner	patrick@puiterwijk.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-25 18:15:00 UTC
Updated	2023-11-07 03:39:00 UTC
Description	Odyssey passes to client unencrypted bytes from man-in-the-middle When Odyssey storage is configured to use the Postgr

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Postgresql	Postgresql	All	All	All	All
Application	Postgresql	Postgresql	14.0	All	All	All

References

Reference	Source	Link	Tags
Issues · yandex/odyssey · GitHub		github.com	
Issues · yandex/odyssey · GitHub	MISC	github.com	
PostgreSQL: CVE-2021-23222: libpq processes unencrypted bytes from man-in-the-middle	MISC	www.postgresql.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[672585](#) EulerOS Security Update for postgresql-10.5 (EulerOS-SA-2023-1346)

[903764](#) Common Base Linux Mariner (CBL-Mariner) Security Update for postgresql (10720)

[904105](#) CBL-Mariner (CBL-Mariner) Security Update for postgresql (140700-1)

© [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](#).

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