



CVE-2021-23222

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

Summary

CVE	CVE-2021-23222
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-02 23:15:00 UTC
Updated	2023-11-07 03:30:00 UTC
Description	A man-in-the-middle attacker can inject false responses to the client's first few queries, despite the use of SSL certificate ve

Risk And Classification

Problem Types: CWE-522

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
git.postgresql.org Git - postgresql.git/commitdiff		git.pos
PostgreSQL: CVE-2021-23222: libpq processes unencrypted bytes from man-in-the-middle	MISC	www.p
libpq: reject extraneous data after SSL or GSS encryption handshake. · postgres/postgres@160c025 · GitHub	MISC	github
2022675 – (CVE-2021-23222) CVE-2021-23222 postgresql: libpq processes unencrypted bytes from man-in-the-middle	MISC	bugzill
PostgreSQL: Multiple Vulnerabilities (GLSA 202211-04) — Gentoo security	GENTOO	securi
git.postgresql.org Git - postgresql.git/commitdiff	MISC	git.pos
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159807 Oracle Enterprise Linux Security Update for libpq (ELSA-2022-1891)
178893 Debian Security Update for postgresql-13 (DSA 5007-1)
178895 Debian Security Update for postgresql-11 (DSA 5006-1)
178897 Debian Security Update for postgresql-9.6 (DLA 2817-1)
198568 Ubuntu Security Notification for PostgreSQL Vulnerabilities (USN-5145-1)
239969 Red Hat Update for rh-postgresql13-postgresql (RHSA-2021:5179)
239972 Red Hat Update for rh-postgresql12-postgresql (RHSA-2021:5197)
240285 Red Hat Update for libpq (RHSA-2022:1891)
282209 Fedora Security Update for pgbouncer (FEDORA-2021-761cda0b77)
357312 Amazon Linux Security Advisory for postgresql : ALAS2POSTGRESQL14-2024-008
357316 Amazon Linux Security Advisory for libpq : ALAS2POSTGRESQL14-2024-009
500544 Alpine Linux Security Update for postgresql
501472 Alpine Linux Security Update for postgresql
501995 Alpine Linux Security Update for postgresql13
502012 Alpine Linux Security Update for postgresql14
502164 Alpine Linux Security Update for postgresql12
502778 Alpine Linux Security Update for postgresql15
504311 Alpine Linux Security Update for postgresql14
671257 EulerOS Security Update for postgresql (EulerOS-SA-2022-1197)
671354 EulerOS Security Update for postgresql (EulerOS-SA-2022-1281)
671698 EulerOS Security Update for postgresql (EulerOS-SA-2022-1756)
690223 Free Berkeley Software Distribution (FreeBSD) Security Update for postgresql (2ccd71bd-426b-11ec-87db-6cc21735f730)
710683 Gentoo Linux PostgreSQL Multiple Vulnerabilities (GLSA 202211-04)
751374 OpenSUSE Security Update for postgresql14 (openSUSE-SU-2021:3759-1)
751375 OpenSUSE Security Update for postgresql13 (openSUSE-SU-2021:3762-1)
751377 OpenSUSE Security Update for postgresql12 (openSUSE-SU-2021:3758-1)
751378 SUSE Enterprise Linux Security Update for postgresql12 (SUSE-SU-2021:3760-1)
751382 SUSE Enterprise Linux Security Update for postgresql96 (SUSE-SU-2021:3757-1)
751386 SUSE Enterprise Linux Security Update for postgresql10 (SUSE-SU-2021:3761-1)

751386 SUSE Enterprise Linux Security Update for postgresql10 (SUSE-SU-2021:3761-1)
751388 SUSE Enterprise Linux Security Update for postgresql, postgresql13, postgresql14 (SUSE-SU-2021:3755-1)
751491 SUSE Enterprise Linux Security Update for postgresql10 (SUSE-SU-2021:4058-1)
751498 OpenSUSE Security Update for postgresql10 (openSUSE-SU-2021:1584-1)
751502 OpenSUSE Security Update for postgresql10 (openSUSE-SU-2021:4058-1)
752505 SUSE Enterprise Linux Security Update for postgresql10 (SUSE-SU-2022:2893-1)
752529 SUSE Enterprise Linux Security Update for postgresql12 (SUSE-SU-2022:2958-1)
900737 Common Base Linux Mariner (CBL-Mariner) Security Update for postgresql (8883)
901728 Common Base Linux Mariner (CBL-Mariner) Security Update for postgresql (8901-1)
940496 AlmaLinux Security Update for libpq (ALSA-2022:1891)
960202 Rocky Linux Security Update for libpq (RLSA-2022:1891)

© [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](#)