



CVE-2024-0985

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

Summary

CVE	CVE-2024-0985
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-02-08 13:15:00 UTC
Updated	2024-03-18 17:15:00 UTC
Description	Description unavailable.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
lists.debian.org/debian-lts-announce/2024/03/msg00017.html		lists.debian.org	
www.postgresql.org/support/security/CVE-2024-0985		www.postgresql.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

- [161373](#) Oracle Enterprise Linux Security Update for postgresql (ELSA-2024-0951)
- [161379](#) Oracle Enterprise Linux Security Update for postgresql:15 (ELSA-2024-0950)
- [161381](#) Oracle Enterprise Linux Security Update for postgresql:13 (ELSA-2024-0975)
- [161383](#) Oracle Enterprise Linux Security Update for postgresql:15 (ELSA-2024-0973)
- [161384](#) Oracle Enterprise Linux Security Update for postgresql:12 (ELSA-2024-0974)

161389 Oracle Enterprise Linux Security Update for postgresql:10 (ELSA-2024-0956)
200140 Ubuntu Security Notification for PostgreSQL Vulnerability (USN-6656-1)
200189 Ubuntu Security Notification for PostgreSQL Vulnerability (USN-6656-2)
242944 Red Hat Update for postgresql:15 (RHSA-2024:0950)
242945 Red Hat Update for postgresql (RHSA-2024:0951)
242946 Red Hat Update for postgresql:10 (RHSA-2024:0956)
242949 Red Hat Update for postgresql:12 (RHSA-2024:0974)
242951 Red Hat Update for postgresql:15 (RHSA-2024:0973)
242961 Red Hat Update for postgresql:13 (RHSA-2024:0975)
242963 Red Hat Update for rh-postgresql13-postgresql (RHSA-2024:0988)
242964 Red Hat Update for rh-postgresql10-postgresql (RHSA-2024:0992)
242968 Red Hat Update for rh-postgresql12-postgresql (RHSA-2024:0990)
242988 Red Hat Update for postgresql:15 (RHSA-2024:1017)
242999 Red Hat Update for postgresql:12 (RHSA-2024:1071)
243002 Red Hat Update for postgresql:12 (RHSA-2024:1070)
243004 Red Hat Update for postgresql:12 (RHSA-2024:1069)
243045 Red Hat Update for postgresql:12 (RHSA-2024:1195)
243047 Red Hat Update for postgresql (RHSA-2024:1241)
243049 Red Hat Update for postgresql (RHSA-2024:1240)
243063 Red Hat Update for postgresql:15 (RHSA-2024:1314)
243067 Red Hat Update for postgresql:13 (RHSA-2024:1315)
243075 Red Hat Update for postgresql:10 (RHSA-2024:1348)
243081 Red Hat Update for postgresql (RHSA-2024:1428)
243082 Red Hat Update for postgresql (RHSA-2024:1426)
243083 Red Hat Update for postgresql (RHSA-2024:1422)
243086 Red Hat Update for postgresql (RHSA-2024:1429)
243103 Red Hat Update for postgresql (RHSA-2024:1437)
357302 Amazon Linux Security Advisory for postgresql15 : ALAS2023-2024-547

357308 Amazon Linux Security Advisory for postgresql : ALAS2POSTGRESQL13-2024-006
357313 Amazon Linux Security Advisory for postgresql : ALAS2POSTGRESQL12-2024-008
357315 Amazon Linux Security Advisory for libpq : ALAS2POSTGRESQL12-2024-009
357320 Amazon Linux Security Advisory for postgresql : ALAS2POSTGRESQL14-2024-006
357321 Amazon Linux Security Advisory for libpq : ALAS2POSTGRESQL14-2024-007
379647 Alibaba Cloud Linux Security Update for postgresql:13 (ALINUX3-SA-2024:0031)
510725 Alpine Linux Security Update for postgresql13
510726 Alpine Linux Security Update for postgresql14
510727 Alpine Linux Security Update for postgresql12
510728 Alpine Linux Security Update for postgresql15
510729 Alpine Linux Security Update for postgresql16
6000476 Debian Security Update for postgresql-15 (DSA 5623-1)
6000478 Debian Security Update for postgresql-13 (DSA 5622-1)
6000529 Debian Security Update for postgresql-11 (DLA 3764-1)
691419 Free Berkeley Software Distribution (FreeBSD) Security Update for postgresql (19e6dd1b-c6a5-11ee-9cd0-6cc21735f730)
755769 SUSE Enterprise Linux Security Update for postgresql15 (SUSE-SU-2024:0520-1)
755773 SUSE Enterprise Linux Security Update for postgresql12 (SUSE-SU-2024:0523-1)
755774 SUSE Enterprise Linux Security Update for postgresql12 (SUSE-SU-2024:0523-1)
755775 SUSE Enterprise Linux Security Update for postgresql12 (SUSE-SU-2024:0523-1)
755776 SUSE Enterprise Linux Security Update for postgresql13 (SUSE-SU-2024:0522-1)
755788 SUSE Enterprise Linux Security Update for postgresql16 (SUSE-SU-2024:0546-1)
755798 SUSE Enterprise Linux Security Update for postgresql14 (SUSE-SU-2024:0552-1)
755799 SUSE Enterprise Linux Security Update for postgresql15 (SUSE-SU-2024:0551-1)
755800 SUSE Enterprise Linux Security Update for postgresql16 (SUSE-SU-2024:0550-1)
755803 SUSE Enterprise Linux Security Update for postgresql12 (SUSE-SU-2024:0542-1)
755804 SUSE Enterprise Linux Security Update for postgresql13 (SUSE-SU-2024:0541-1)
755805 SUSE Enterprise Linux Security Update for postgresql14 (SUSE-SU-2024:0540-1)
908025 Common Base Linux Mariner (CBL-Mariner) Security Update for postgresql (34279-1)
941591 AlmaLinux Security Update for postgresql:12 (ALSA-2024:0974)

941592 AlmaLinux Security Update for postgresql:13 (ALSA-2024:0975)
941594 AlmaLinux Security Update for postgresql:15 (ALSA-2024:0973)
941598 AlmaLinux Security Update for postgresql:10 (ALSA-2024:0956)
941599 AlmaLinux Security Update for postgresql:15 (ALSA-2024:0950)
941603 AlmaLinux Security Update for postgresql (ALSA-2024:0951)
961120 Rocky Linux Security Update for postgresql:10 (RLSA-2024:0956)
961123 Rocky Linux Security Update for postgresql:15 (RLSA-2024:0950)
961125 Rocky Linux Security Update for postgresql:13 (RLSA-2024:0975)
961129 Rocky Linux Security Update for postgresql:15 (RLSA-2024:0973)

© [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](#)