CVE-2021-23214

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-23214
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-04 16:15:00 UTC
Updated	2023-11-07 03:30:00 UTC
Description	When the server is configured to use trust authentication with a clientcert requirement or to use cert authentication, a man-i

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Postgresql	Postgresql	All	All	All	All
Application	Postgresql	Postgresql	14.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	8.0	All	All	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	8.0	All	All	All
Application	Redhat	Software Collections	1.0	All	All	All

References

Reference	Source	Link
Reject extraneous data after SSL or GSS encryption handshake. · postgres/postgres@28e2412 · GitHub	MISC	githu
PostgreSQL: CVE-2021-23214: Server processes unencrypted bytes from man-in-the-middle	MISC	www
git.postgresql.org Git - postgresql.git/commit		git.p
git.postgresql.org Git - postgresql.git/commit	MISC	git.p
2022666 – (CVE-2021-23214) CVE-2021-23214 postgresql: server processes unencrypted bytes from man-in-the-middle	MISC	bugz
PostgreSQL: Multiple Vulnerabilities (GLSA 202211-04) — Gentoo security	GENTOO	secu

CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.r

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159576 Oracle Enterprise Linux Security Update for postgresql:12 (ELSA-2021-5235)
- 159577 Oracle Enterprise Linux Security Update for postgresql:13 (ELSA-2021-5236)
- 159822 Oracle Enterprise Linux Security Update for postgresql:10 (ELSA-2022-1830)
- 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)
- 239975 Red Hat Update for postgresql:13 (RHSA-2021:5236)
- 239976 Red Hat Update for postgresql:12 (RHSA-2021:5235)
- 240308 Red Hat Update for postgresql:10 (RHSA-2022:1830)
- 282209 Fedora Security Update for pgbouncer (FEDORA-2021-761cda0b77)
- 354679 Amazon Linux Security Advisory for postgresql93 : ALAS-2023-1658
- 354682 Amazon Linux Security Advisory for postgresql96 : ALAS-2023-1661
- 354683 Amazon Linux Security Advisory for postgresql92 : ALAS-2023-1657
- 354685 Amazon Linux Security Advisory for postgresql95 : ALAS-2023-1660
- 354687 Amazon Linux Security Advisory for postgresql94 : ALAS-2023-1659
- 354761 Amazon Linux Security Advisory for postgresql : ALAS2-2023-1949
- 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

671231 EulerOS Security Update for postgresql (EulerOS-SA-2022-1182)

671354 EulerOS Security Update for postgresql (EulerOS-SA-2022-1281)

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)

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)

900743 Common Base Linux Mariner (CBL-Mariner) Security Update for postgresql (8955)

900921 Common Base Linux Mariner (CBL-Mariner) Security Update for postgresql (8973-1)

940094 AlmaLinux Security Update for postgresql:12 (ALSA-2021:5235)

940417 AlmaLinux Security Update for postgresql:13 (ALSA-2021:5236)

940528 AlmaLinux Security Update for postgresql:10 (ALSA-2022:1830)

960321 Rocky Linux Security Update for postgresql:13 (RLSA-2021:5236)

960337 Rocky Linux Security Update for postgresql:12 (RLSA-2021:5235)

960350 Rocky Linux Security Update for postgresql:10 (RLSA-2022:1830)

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