



CVE-2020-14349

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

Summary

CVE	CVE-2020-14349
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-24 13:15:00 UTC
Updated	2023-01-24 02:22:00 UTC
Description	It was found that PostgreSQL versions before 12.4, before 11.9 and before 10.14 did not properly sanitize the search_path

Risk And Classification

Problem Types: CWE-89 | CWE-427

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Postgresql	Postgresql	All	All	All	All
Application	Postgresql	Postgresql	All	All	All	All

References

Reference	Source	Link
August 2020 PostgreSQL Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.ne
PostgreSQL: Multiple vulnerabilities (GLSA 202008-13) — Gentoo security	GENTOO	security.ge
[security-announce] openSUSE-SU-2020:1243-1: important: Security update	SUSE	lists.opens
[security-announce] openSUSE-SU-2020:1312-1: important: Security update	SUSE	lists.opens
[security-announce] openSUSE-SU-2020:1244-1: important: Security update	SUSE	lists.opens
1865744 – (CVE-2020-14349) CVE-2020-14349 postgresql: Uncontrolled search path element in logical replication	MISC	bugzilla.re
USN-4472-1: PostgreSQL vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu
[security-announce] openSUSE-SU-2020:1326-1: important: Security update	SUSE	lists.opens

[security-announce] openSUSE-SU-2020:1228-1: moderate: Security update f	SUSE	lists.opensuse.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159270](#) Oracle Enterprise Linux Security Update for rh-postgresql10-postgresql (ELSA-2021-9290)

[377113](#) Alibaba Cloud Linux Security Update for postgresql:12 (ALINUX3-SA-2021:0017)

[500539](#) Alpine Linux Security Update for postgresql

[502007](#) Alpine Linux Security Update for postgresql14

[502161](#) Alpine Linux Security Update for postgresql12

[502773](#) Alpine Linux Security Update for postgresql15

[504306](#) Alpine Linux Security Update for postgresql14

[900047](#) CBL-Mariner Linux Security Update for postgresql 12.1

[902841](#) Common Base Linux Mariner (CBL-Mariner) Security Update for postgresql (2011)

[940130](#) AlmaLinux Security Update for postgresql:12 (ALSA-2020:5620)

[960242](#) Rocky Linux Security Update for postgresql:12 (RLSA-2020:5620)

© [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](#)