PostgreSQL fixes 52 vulnerabilities: why this update needs more than a restart

18 November 2026 · 5 min read · blogs.iictp.org/postgresql-november-2026-security-release-post-update-steps

The PostgreSQL Global Development Group released PostgreSQL 18.7, 17.12, 16.16, 15.20 and 14.25 on 12 November 2026, along with the second release candidate of PostgreSQL 19. The project says the release fixes 52 security vulnerabilities and over 140 bugs, and that several issues may require extra steps after updating.

TL;DR The short version

- PostgreSQL's 12 November 2026 minor releases fix 52 security vulnerabilities and over 140 bugs.
- Many flaws score 8.8 on CVSS, and some are in client tools such as pg_dump, so servers alone are not enough.
- No dump and reload is needed, but update client tools on every host, including backup servers, and check the extra post-update steps.

Read online, listen to it, or change the text size: https://blogs.iictp.org/postgresql-november-2026-security-release-post-update-steps

What was reported

- Many of the listed vulnerabilities carry a CVSS v3.1 score of 8.8, including type-confusion and use-after-free flaws that the announcement says can execute arbitrary code.
- The list also covers client tools. Examples include SQL injection through pg_dump constraint names and arbitrary code execution in pg_restore through missing validation of non-plain archives.
- Bug fixes address GIN and pg_trgm GiST index problems that could make queries miss rows, and incremental backup problems that could produce corrupt backups.
- This is the final release of PostgreSQL 14, which the project says is now end-of-life and will receive no further security or bug fixes.
- The announcement gives 19 November 2026 as the planned general availability date for PostgreSQL 19.

What a practitioner should do

- Schedule the minor update. The project says no dump and reload or pg_upgrade is needed: stop PostgreSQL and update its binaries.
- Update client tools too, on every host that runs pg_dump, pg_restore or similar utilities, including backup servers.

- Reindex where the announcement says to: GiST indexes using gist_trgm_ops, B-tree indexes on bpchar columns declared without a length, and any GIN index you suspect is affected. If you see missing chunk number errors, reindex the table.
- If you use incremental backups, take a new full backup after updating and use it as the base for later incrementals, as the project recommends.
- If you use partitioned tables, run the query in the announcement to find NOT NULL NO INHERIT constraints, then drop or repair them.
- If you skipped earlier updates, read the release notes for those versions too, since they may add further steps. Start planning an upgrade for anything still on PostgreSQL 14.

The wider lesson

A patch is not finished when the binary changes. Data repairs, fresh backups and client tools are part of the same change, and a runbook should say so. Testing that a restore works after this kind of update is the sort of verification the Infrastructure & Security domain of the TPBOK encourages.

> Facts in this post were read from the sources listed below on 18 November 2026; this is a developing story or product and details may have changed since.

Sources and further reading

1. PostgreSQL Global Development Group. PostgreSQL 18.7, 17.12, 16.16, 15.20, 14.25, and 19 RC 2 Released! 12 November 2026. postgresql.org/about/news/postgresql-187-1712-1616-1520-1425-and-19-rc-2-released-3442/

Published by IICTP, an independent technical credential body, on 18 November 2026. The current version of this post is at https://blogs.iictp.org/postgresql-november-2026-security-release-post-update-steps. More guides: blogs.iictp.org.