AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Përditësime të Sigurisë - PostgreSQL

Data: 19/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

PostgreSQL ka publikuar përditësime sigurie për të adresuar dobësi të shumta në produktet e saj.

Informacione Teknike

Grupi Global i Zhvillimit PostgreSQL ka publikuar përditësime sigurie për të gjitha versionet e mbështetura të PostgreSQL. Ky publikim adreson pesë dobësi sigurie, duke përfshirë zbulimin e kujtesës dhe probleme të shumta me ekzekutimin e kodit arbitrar.

Detajet e dobësive
Dobësi të Ashpërsisë së Lartë
• CVE-2026-2004 – ekzekutimi arbitrar i kodit intarray
Dështimi për të validuar llojet e hyrjes në funksionin e vlerësuesit të selektivitetit të zgjerimit intarray mund të lejojë një krijues objekti të ekzekutojë kod arbitrar si përdorues i sistemit operativ që ekzekuton bazën e të dhënave.
• CVE-2026-2005 – mbingarkesa e buferit të grumbullit pgcrypto
Një mbingarkesë e buferit të grumbullit në pgcrypto lejon një ofrues të tekstit të shifruar të ekzekutojë kod arbitrar si përdorues i sistemit operativ që ekzekuton bazën e të dhënave.
• CVE-2026-2006 – validimi i karaktereve ekzekutimi arbitrar i kodi
Mungesa e validimit të gjatësive të karaktereve shumëbajtëshe në funksionet e manipulimit të tekstit lejon që pyetjet e hartuara të shkaktojnë një tejkalim të buferit, duke rezultuar në ekzekutimin arbitrar të kodit
• CVE-2026-2007 – mbingarkesë e buferit të grumbullit pg_trgm
Një mbingarkesë e buferit të grumbullit në pg_trgm i lejon një përdoruesi të bazës së të dhënave të shkruajë të dhëna modeli në memorien e serverit. Përshkallëzimi i mundshëm i privilegjeve nuk mund të përjashtohet.

Dobësi e Ashpërsisë së Mesme
• CVE-2026-2003 – zbulimi i memories oidvector
Validimi i gabuar i tipit oidvector i lejon një përdoruesi të bazës së të dhënave të zbulojë disa bajt të memories së serverit. Edhe pse mundësia e rrjedhjes së informacionit të ndjeshëm është e ulët, kjo dobësi teorikisht mund të ekspozojë të dhëna konfidenciale.

Ndikimi
Shfrytëzimi i suksesshëm i këtyre dobësive mund të lejojë një sulmues të ekzekutojë kod arbitrar me privilegjet e serverit të bazës së të dhënave dhe të shkaktojë rrëzime ose korruptim të memories. Këto probleme paraqesin një rrezik të lartë për konfidencialitetin, integritetin dhe disponueshmërinë e sistemeve të prekura,

Versionet e përditësuara:
• PostgreSQL 18.2, 17.8, 16.12, 15.16 dhe 14.21

Rekomandime

AKSK rekomandon të përditësoni PostgreSQL në versionin e fundit