DBOD public schema access review

Maurizio De Giorgi

14 August 2024

DBOD public schema access review 1/3: the issue

It all began with CVE-2018-1058[1]:

- ...*describes how a user can create like-named objects in different schemas that can change the behavior of other users' queries and cause unexpected or malicious behavior, also known as a* "trojan-horse" attack
- ...explains which PostgreSQL installations are likely to be affected
- *...indicates some* ways to protect your PostgreSQL installation [2]

1 A Guide to CVE-2018-1058: Protect Your Search Path

2 5.9.6 Usage Patterns

DBOD public schema access review 2/3: actions

- Do not allow users to create new objects in the public schema
  - Default for new instances PG 15+
  - Recommended action (after testing) for existing instances (PG 13, 14):
    - `REVOKE CREATE ON SCHEMA public FROM PUBLIC`
- Recommended actions (after testing) for ALL instances:
  - Remove the public schema from the default search_path at run-time
    - `ALTER ROLE all SET search_path = "$user"`
  - Remove public schema from default search_path in postgresql.conf
    - `search_path = '"$user"'`

DBOD public schema access review 3/3: summary

New instances (PG15+)

- New default, coming out-of-the-box, adopted by DBOD team:
  - `REVOKE CREATE ON SCHEMA public FROM PUBLIC`

Existing instances (PG 13, 14) and Upgraded instances (also to PG15+)

- Nothing changed by DBOD team
- We recommend the actions in previous slide (owners take responsibility)
- 3-scheme based system (next slide) for new projects or complete refactoring:
  - Improved security, human errors risks mitigation
  - Based on Principle of Least Privilege and role-based separation
  - Used in DBOD main database: get in touch for any question and know more

DBOD 3-scheme based system