DB on Demand secure schema usage patterns for PostgreSQL

Maurizio De Giorgi

Date

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

> ...*which 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*

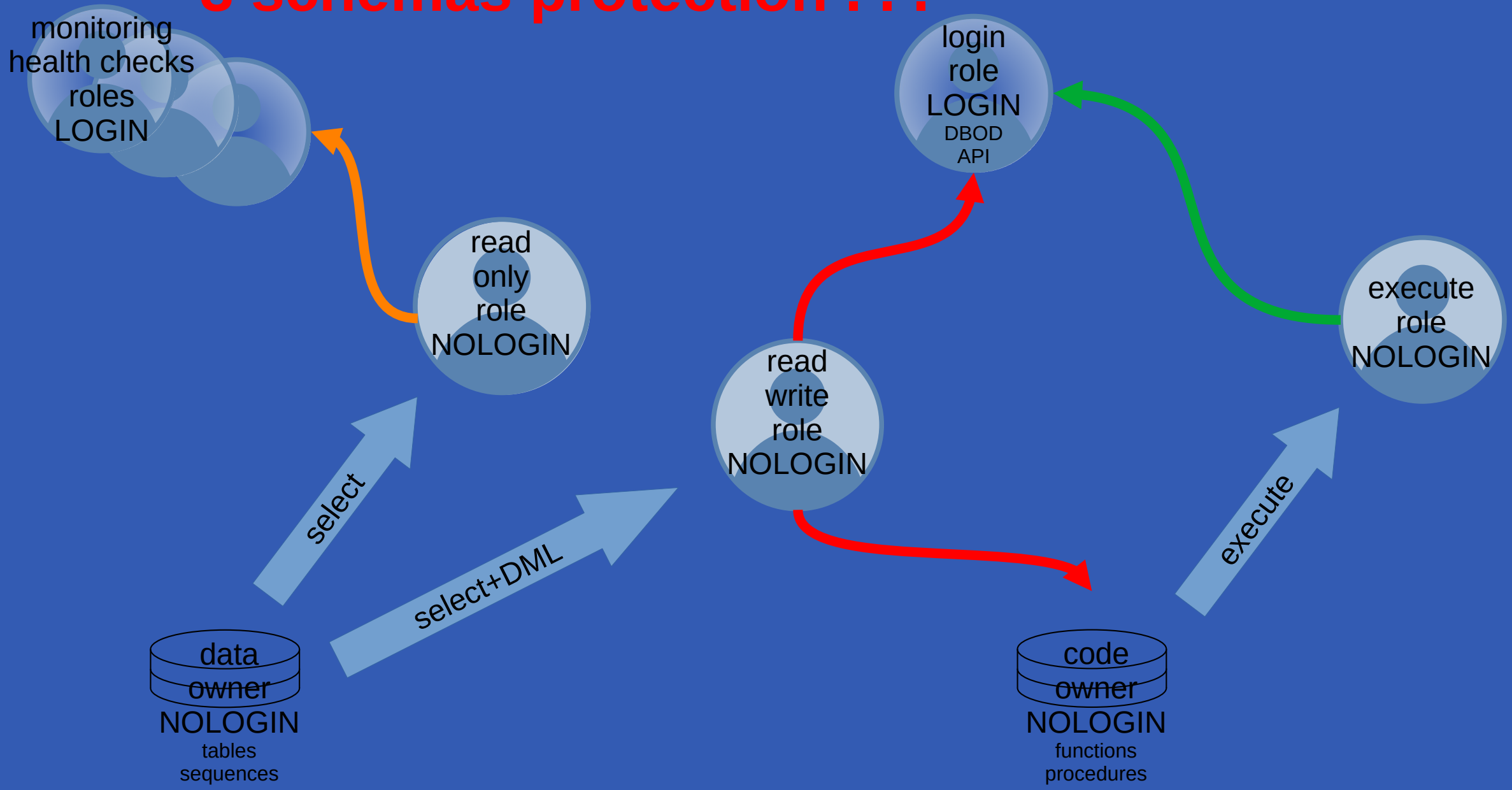
> *...indicates some ways to protect your PostgreSQL installation (see also PG docs[2])*

- Do not allow users to create new objects in the public schema (default in PG 15)
  `REVOKE CREATE ON SCHEMA public FROM PUBLIC`
- Remove the public schema from the default search_path at run-time
  `ALTER ROLE all SET search_path = "$user"`
- Remove the public schema from the default search_path in postgresql.conf
  `search_path = '"$user"'`

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

2 5.9.6 Usage Patterns

3 schemas protection . . .



What we plan to do

New instances (PG15+)

- Adopt the new default (remove access to public)
- Remove the public schema from the default search_path in postgresql.conf
  `search_path = '"$user"'`
- Deploy 3 schemas and related roles ready to be used

Existing instances (PG 13, 14)

- Explain and document protection measures deployment, owner take responsibility

Upgraded instances (to PG15+)

- Automate protection measures deployment as part of the upgrade