Database Configuration Security Compliance

2024-05-12 23:39

Tested System Information

Path to PostgreSQL Configuration: C:\Program Files\PostgreSQL\16\data
Database Name: experimental_db
User: postgres
Host: localhost
Port: 5432
CPU: Intel64 Family 6 Model 165 Stepping 2, GenuineIntel (4 cores)
RAM: 7 GB
Storage Size: 59 GB
Operating System: Windows 10
PostgreSQL Version: 16.2

1 Tested areas

No.	area of interest	tested	compliant	severity
1	LTS - Encryption at REST/transit	✓	×	low
2	Insecure authentication methods	✓	✓	medium
3	Trust authentication	✓	✓	high
4	Supported version of PostgreSQL	✓	✓	low
5	Permissions test	✓	×	info
6	Check pgcrypto	✓	×	low
7	Role pg_execute_server_program enabled	✓	✓	info
8	SQL server allowed to read or write operating system files	✓	×	info
9	Log configuration	✓	×	info
10	Client side errors	✓	×	low
11	Configuration of SSL	✓	×	medium
12	Unlimited superuser access	✓	×	info

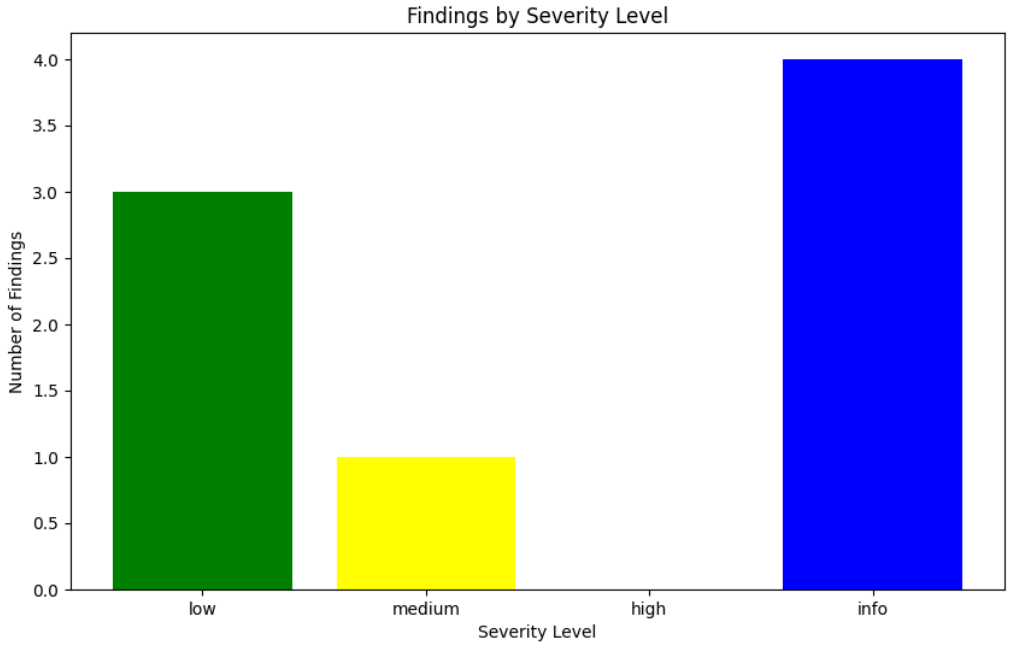
2 Disclaimer

Please note that the test results provided have been generated automatically and while every effort has been made to ensure accuracy, there may be errors or omissions that were not detected during the automated process. Users are encouraged to critically review these results and consider them as part of a broader assessment. It is important to understand that automated tests are not a substitute for human oversight, and manual verification of findings is recommended wherever possible. Although the system is designed to be precise, it is not infallible, and instances of false positives or negatives may occur. The system and its algorithms are subject to regular updates, meaning that results may vary over time with improvements in technology. Additionally, this automated test might not cover all aspects of the subject matter, and additional analysis may be required for a more thorough understanding. Users should be aware that they assume all responsibility for any actions taken based on these results and that we are not liable for any direct or indirect consequences arising from their use. By using these results, you acknowledge and agree to these limitations.

3 Summary

During the test total of 8 misconfigurations were found.

Following figure shows graphically number of misconfigurations and their impact:



4 Technical details

4.1 LTS - Encryption at REST/transit

Description This test verifies that database enforces encryption to ensure safe communication that cannot be eavesdropped. Improper configuration of encryption could lead to violation of CIA triade.

This test found that following databases are not configured to ensure encrypted communication:

TYPE	DATABASE	USER	ADDRESS	METHOD
host	all	all	127.0.0.1/32	scram-sha-256
host	all	all	::1/128	scram-sha-256
host	replication	all	127.0.0.1/32	scram-sha-256
host	replication	all	::1/128	scram-sha-256

Recommendation We recoment implementing secure data transit with encryption.

4.2 Insecure authentication methods

Description This test examines the configuration file 'pg_hba.conf' for the presence of insecure authentication methods. Specifically, it identifies the use of 'md5' and 'password' methods, both of which are considered insecure. The 'md5' method employs a deprecated hash function that has been cryptographically compromised, while the 'password' method transmits credentials in plaintext, posing significant security risks.

Database uses configuration that enforce secure authentication methods

4.3 Trust authentication

Description Trust authentication permits unrestricted access to the database for any user without requiring a password. This configuration poses a significant security risk, as it allows potentially unauthorized individuals to gain access to sensitive data and perform unauthorized actions within the database. Utilizing trust authentication undermines the fundamental principle of access control and compromises the confidentiality, integrity, and availability of the database.

User cannot connect without authentication.

4.4 Supported version of PostgreSQL

Description This test verifies whether the database uses the latest software version. Outdated versions could contain security vulnerabilities that could be used by an attacker to compromise the database.

Database uses latest version of PostgreSQL.

4.5 Permissions test

Description The following table provides a comprehensive overview of all privileges assigned within the specified database. This information is crucial for evaluating the access control mechanisms in place and identifying potential security vulnerabilities. A thorough permissions audit ensures that only authorized users have appropriate access rights, minimizing the risk of unauthorized data access or modification. Following table contains users and their permission on database tables:

User Type	Table Schema	Table Name	Privilege Types
public_user	my_schema	public_info	SELECT
private_user	my_schema	public_info	SELECT
private_user	my_schema	private_info	SELECT
admin_user	my_schema	public_info	INSERT, SELECT, UPDATE, DELETE
admin_user	my_schema	private_info	INSERT, SELECT, UPDATE, DELETE
admin_user	my_schema	secret_info	INSERT, SELECT, UPDATE, DELETE

4.6 Check pgcrypto

Description Verifies whether the database is capable of encrypting its data on database layer.

Database does not implement the pg_crypto crypto extension, be installed using the `CREATE EXTENSION IF NOT EXISTS pgcrypto;`. Full guide on how to use this extension can be found on `https://www.postgresql.org/docs/current/pgcrypto.html`.

4.7 Role pg_execute_server_program enabled

Description Verifies that no user has role that enables command execution.

No users with pg_execute_server_program were found.

4.8 SQL server allowed to read or write operating system files

Description Tests whether the database is able to access OS files.

Test was able to read postgresql.conf from SQL query

4.9 Log configuration

Description Verifies that the log configuration is correct.

Configuration Name	DB Setting	Recommended Setting	Compliant
log_statement	N/A	ddl	×
log_duration	N/A	on	×
log_min_duration_statement	N/A	0	×
log_connections	N/A	on	×
log_disconnections	N/A	on	×
log_lock_waits	N/A	on	×
log_temp_files	N/A	0	×

4.10 Client side errors

Description Verifies that the database doesnt return errors to the client side.

Aplication does not set up parameters for verbosity of errors.

4.11 Configuration of SSL

Description Verifies that has the correct ssl configuration in postgres.conf

Configuration Name	DB Setting	Recommended Setting	Compliant
ssl	N/A	on	×
ssl_cert_file	N/A	<cert file>	×
ssl_key_file	N/A	<key file>	×
ssl_ca_file	N/A	<root cert file>	×
ssl_prefer_server_ciphers	N/A	on	×

4.12 Unlimited superuser access

Description This test checks superuser accounts, and verifies whether they have limited access or not.

- admin_user - Access to all tables: Yes