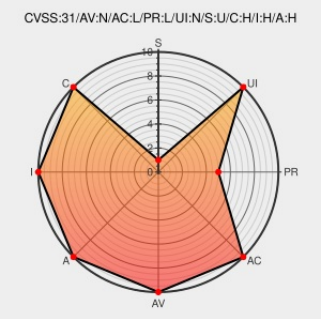
CVE-2023-25149

Published on: Not Yet Published

Last Modified on: 02/22/2023 07:09:00 PM UTC

CVE-2023-25149 - advisory for GHSA-44jh-j22r-33wq

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Timescaledb from Timescale contain the following vulnerability:

TimescaleDB, an open-source time-series SQL database, has a privilege escalation vulnerability in versions 2.8.0 through 2.9.2. During installation, TimescaleDB creates a telemetry job that is runs as the installation user. The queries run as part of the telemetry data collection were not run with a locked down `search_path`, allowing malicious users to create functions that would be executed by the telemetry job, leading to privilege escalation. In order to be able to take advantage of this vulnerability, a user would need to be able to create objects in a database and then get a superuser to install TimescaleDB into their database. When TimescaleDB is installed as trusted extension, non-superusers can install the extension without help from a superuser. Version 2.9.3 fixes this issue. As a mitigation, the `search_path` of the user running the telemetry job can be locked down to not include schemas writable by other users. The vulnerability is not exploitable on instances in Timescale Cloud and Managed Service for TimescaleDB due to additional security provisions in place on those platforms.

CVE-2023-25149 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **timescale** - **timescaledb** version **= >= 2.8.0, < 2.9.3**

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link

TimescaleDB 2.8.0 through 2.9.2 has incorrect access control · Advisory · timescale/timescaledb · GitHub	github.com text/html	MISC github.com/timescale/timescaledb/security/advisories/GHSA-44jh-j22r-33wq
Release 2.9.3 (2023-02-06) · timescale/timescaledb · GitHub	github.com text/html	MISC github.com/timescale/timescaledb/releases/tag/2.9.3
Lock down search_path in SPI calls by svenklemm · Pull Request #5259 · timescale/timescaledb · GitHub	github.com text/html	MISC github.com/timescale/timescaledb/pull/5259

Related QID Numbers

503218 Alpine Linux Security Update for postgresql-timescaledb

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Timescale	Timescaledb	All	All	All	All

cpe:2.3:a:timescale:timescaledb:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2023-25149	2023-02-14 15:38:28

← Previous ID

Next ID→