

# Fujitsu Enterprise Postgres

## Urgent notification

Global Support News and IMPORTANT update information - No. GSI26-H005-01

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability [CVE-2026-2007](#) reported by OSS PostgreSQL community.

[CVE-](#)

Fujitsu Limited

February 13, 2026

### Incident Information

[Incident management number] PH25098

- Description:

pg\_trgm may cause buffer overrun.

This is CVE-2026-2007 vulnerability reported by PostgreSQL community.

- Products and versions affected:

**Version 18:**

Fujitsu Enterprise Postgres Advanced Edition 18 for Linux

Fujitsu Enterprise Postgres Advanced Edition 18 for Windows

Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 18 for Linux

Fujitsu Enterprise Postgres Standard Edition 18 for Linux

Fujitsu Enterprise Postgres Standard Edition 18 for Windows

Fujitsu Enterprise Postgres Advanced Edition 18 Operator Bundle for Kubernetes

Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 18 for Kubernetes

Report classification	<input checked="" type="checkbox"/> Incident	<input type="checkbox"/> Degradation (EVL-UP)	<input type="checkbox"/> Cautions
	<input type="checkbox"/> Application recommended		
Impact on operation	The server is attacked by buffer overrun attacks.		
Recovery tasks	<input type="checkbox"/> Required	<input checked="" type="checkbox"/> Not required	
Occurrence frequency	<input checked="" type="checkbox"/> Always	<input type="checkbox"/> Rarely	<input type="checkbox"/> Random
	<input type="checkbox"/> Other ()		

## Detailed Information

### 1. Issue and conditions to reproduce issue

[Issue]

pg\_trgm may cause buffer overrun.

[Environment]

- Linux
- Windows

[Conditions]

- 1) Use pg\_trgm. AND
- 2) Perform lowercasing.

### 2. Cause

There were issues in pg\_trgm.

### 3. How to avoid the issue

Apply patch when released by Fujitsu.

A community patch (for version 14-18) will be released soon, and a corresponding Fujitsu Enterprise Postgres patch (for version 14-18) to follow. A notification will be sent to when the patch is made available.

Contact your Fujitsu service support center.

[Workaround]

None.

### 4. Recovery measures after the issue occurs

None.

### 5. Other

None.

[Revision history]

First edition

© Fujitsu 2026. All rights reserved. Fujitsu and Fujitsu logo are trademarks of Fujitsu Limited registered in many jurisdictions worldwide. Other product, service and company names mentioned herein may be trademarks of Fujitsu or other companies. This document is current as of the initial date of publication and subject to be changed by Fujitsu without notice. This material is provided for information purposes only and Fujitsu assumes no liability related to its use.