

Fujitsu Enterprise Postgres

Urgent notification

Global Support News and IMPORTANT update information - No. GSI26-H018-02

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability [CVE-2026-17346](#) reported by pgAdmin4 community.

Fujitsu Limited

September 9, 2026

Incident Information

[Incident management number] PH25533

- Description:

In pgAdmin4, there was a bug in the SQL templates used to display the Statistics tab for indexes and the Dependencies tab for publications and subscriptions, where object names (table names, index names, publication names, and subscription names) were embedded directly into SQL statements without being properly escaped.

A low-privileged user with CREATE TABLE, CREATE PUBLICATION, and CREATE SUBSCRIPTION privileges could create a specially crafted object name, which could then be exploited to execute arbitrary SQL using the database privileges of another user viewing that object within their pgAdmin4 session.

This is CVE-2026-17346 vulnerability reported by pgAdmin4 community.

- Products and versions affected:

Version 12:

FUJITSU Enterprise Postgres Client 12/12SP1/12SP1B for Windows

Version 13:

FUJITSU Enterprise Postgres Client 13/13SP1/13SP1A for Windows

Version 14:

FUJITSU Enterprise Postgres Client 14/14A/14SP1 for Windows

Version 15:

Fujitsu Enterprise Postgres Client 15/15SP1/15SP2 for Windows

Fujitsu Enterprise Postgres Client with Cryptographic Module 15 for Windows

Version 16:

Fujitsu Enterprise Postgres Client 16/16SP1 for Windows

Fujitsu Enterprise Postgres Client with Cryptographic Module 16 for Windows

Version 17:

Fujitsu Enterprise Postgres Client 17/17SP1/17SP2 for Windows

Fujitsu Enterprise Postgres Client with Cryptographic Module 17 for Windows

Version 18:

Fujitsu Enterprise Postgres Client 18/18SP1/18SP2 for Windows

Fujitsu Enterprise Postgres Client with Cryptographic Module 18 for Windows

Report classification	☒ Incident ☐ Application recommended	☐ Degradation (EVL-UP)	☐ Cautions
Impact on operation	Arbitrary SQL execution under the viewing user's privileges via maliciously named database objects.		
Recovery tasks	☐ Required	☒ Not required	
Occurrence frequency	☒ Always ☐ Other ()	☐ Rarely	☐ Random
Workaround	☐ Yes	☒ No	

Detailed Information

1. Issue and conditions to reproduce issue

[Issue]

In pgAdmin4, there was a bug in the SQL templates used to display the “Statistics” tab for indexes and the “Dependencies” tab for publications and subscriptions, where object names (table names, index names, publication names, and subscription names) were embedded directly into SQL statements without being properly escaped.

A low-privileged user with CREATE TABLE, CREATE PUBLICATION, and CREATE SUBSCRIPTION privileges could create a specially crafted object name, which could then be exploited to execute arbitrary SQL using the database privileges of another user viewing that object within their pgAdmin4 session.

[Environment]

- Windows

[Conditions]

1) When you open the "Statistics" tab for an index or the "Dependencies" tab for a publication or subscription in pgAdmin4.

2. Cause

There were issues with object names not being properly escaped before being inserted into SQL templates.

3. How to avoid the issue

Apply patch when released by Fujitsu.

A community patch has been released, 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]

Second 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.