# Fujitsu Enterprise Postgres

Urgent notification

**Global Support News and IMPORTANT update information - No. GSI26-H019-01**

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability CVE-2026-17566 reported by pgAdmin4 community.

Fujitsu Limited

August 3, 2026

## Incident Information

[Incident management number] PH25533

- Description:

  In pgAdmin4's Import/Export tool, there was a flaw in the validation process used when exporting data via a query.

  By exploiting a mismatch in backslash-escape interpretation with psql's default standard_conforming_strings = on behavior, a crafted query string could bypass the parenthesis-balance check in the \copy (...) command, exposing a live TO PROGRAM clause that allows arbitrary OS command execution.

  This is CVE-2026-17566 vulnerability reported by pgAdmin4 community.

- Products and versions affected:

  **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 2026

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 | [x] Incident<br>[] Application recommended | [] Degradation (EVL-UP) | [] Cautions |
| Impact on operation | Arbitrary OS command execution via a crafted export query. | | |
| Recovery tasks | [] Required | [x] Not required | |
| Occurrence frequency | [x] Always<br>[] Other () | [] Rarely | [] Random |
| Workaround | [] Yes | [x] No | |

## Detailed Information

1. Issue and conditions to reproduce issue

   [Issue]

   In pgAdmin4's Import/Export tool, there was a flaw in the validation process used when exporting data via a query.

   By exploiting a mismatch in backslash-escape interpretation with psql's default standard_conforming_strings = on behavior, a crafted query string could bypass the parenthesis-balance check in the \copy (...) command, exposing a live TO PROGRAM clause that allows arbitrary OS command execution.

   [Environment]

   - Windows

   [Conditions]

   1) When using Export Data Using Query in the Import/Export tool. AND

   2) Specially crafted SQL query containing a backslash within a single-quote string is specified as the target for export.

2. Cause

   There was an issue with the export-query guard misjudging backslash-escaping.

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.

 © Fujitsu 2026

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.