Fujitsu Enterprise Postgres

Urgent notification

Global Support News and IMPORTANT update information - No. GSI26-H048-02

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability CVE-2026-86861 reported by OSS PgAdmin4 community.

Fujitsu Limited

Oct 28, 2026

Incident Information

[Incident management number] PH25599

- **Description:**

  In pgAdmin4, if a symbolic link is replaced between the access permission check and the file write, protection of the write target may be insufficient and a write to an unintended file may be performed in Storage Manager.

  As a result, in an environment where an attacker can place a crafted symbolic link at the conflict timing, an arbitrary file overwrite may occur.

  This is CVE-2026-86861 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 2026

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	[x] Incident [] Application recommended	[] Degradation (EVL-UP)	[] Cautions
Impact on operation	An arbitrary file overwrite may occur.		
Recovery tasks	[] Required	[x] Not required	
Occurrence frequency	[x] Always [] Other ()	[] Rarely	[] Random
Workaround	[] Yes	[x] No	

Detailed Information

1. Issue and conditions to reproduce issue

[Issue]

In pgAdmin4, if a symbolic link is replaced between the access permission check and the file write, protection of the write target may be insufficient and a write to an unintended file may be performed in Storage Manager.

As a result, in an environment where an attacker can place a crafted symbolic link at the conflict timing, an arbitrary file overwrite may occur.

[Environment]

- Windows

[Conditions]

1) A file save operation is performed in Storage Manager. AND

2) The final component of the save destination is replaced with a symbolic link after the check.

2. Cause

There were issues in symbolic link replacement between the access permission check and the file write.

3. How to avoid the issue

 © Fujitsu 2026

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.