Fujitsu Enterprise Postgres

Urgent notification

Global Support News and IMPORTANT update information - No. GSI26-H002-02

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability CVE-2026-2004 reported by OSS PostgreSQL community.

Fujitsu Limited

October 28, 2026

Incident Information

[Incident management number] PH25094, PH25095, PH25096, PH25097, PH25098, PH25213

- **Description:**

  Manipulated input may cause arbitrary code execution when using selectivity estimation function.

  This is CVE-2026-2004 vulnerability reported by PostgreSQL community.

- **Products and versions affected:**

  Version 12:

  FUJITSU Enterprise Postgres Advanced Edition 12/12SP1/12SP1A/12SP1B for Linux

  FUJITSU Enterprise Postgres Advanced Edition 12/12SP1/12SP1A/12SP1B for Windows

  FUJITSU Enterprise Postgres Standard Edition 12/12SP1/12SP1A/12SP1B for Linux

  FUJITSU Enterprise Postgres Standard Edition 12/12SP1/12SP1A/12SP1B for Windows

  Version 13:

  FUJITSU Enterprise Postgres Advanced Edition 13/13SP1/13SP1A for Linux

  FUJITSU Enterprise Postgres Advanced Edition 13/13SP1/13SP1A for Windows

  FUJITSU Enterprise Postgres Standard Edition 13/13SP1/13SP1A for Linux

  FUJITSU Enterprise Postgres Standard Edition 13/13SP1/13SP1A for Windows

  Version 14:

  FUJITSU Enterprise Postgres Advanced Edition 14/14SP1 for Linux

  FUJITSU Enterprise Postgres Advanced Edition 14 for Windows

  FUJITSU Enterprise Postgres Advanced Edition 14/14SP1 for Linux on Z

  FUJITSU Enterprise Postgres Advanced Edition 14/14SP1 for Linux on IBM Power(R)

 © Fujitsu 2026

FUJITSU Enterprise Postgres Standard Edition 14 for Linux
FUJITSU Enterprise Postgres Standard Edition 14 for Windows
FUJITSU Enterprise Postgres Advanced Edition 14/14SP1 Operator Bundle for Kubernetes
FUJITSU Enterprise Postgres Advanced Edition 14/14SP1 Operator Bundle for Kubernetes on Z
FUJITSU Enterprise Postgres Advanced Edition 14/14SP1 Operator Bundle for Kubernetes on IBM Power(R)

Version 15:

Fujitsu Enterprise Postgres Advanced Edition 15/15SP1/15SP2 for Linux
Fujitsu Enterprise Postgres Advanced Edition 15 for Windows
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 15 for Linux
Fujitsu Enterprise Postgres Advanced Edition 15/15SP1/15SP2 for Linux on Z
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 15 for Linux on Z
Fujitsu Enterprise Postgres Advanced Edition 15 for Linux on IBM Power(R)
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 15 for Linux on IBM Power(R)
Fujitsu Enterprise Postgres Standard Edition 15/15SP1 for Linux
Fujitsu Enterprise Postgres Standard Edition 15 for Windows
Fujitsu Enterprise Postgres Advanced Edition 15/15SP1/15SP2 Operator Bundle for Kubernetes
Fujitsu Enterprise Postgres Advanced Edition 15/15SP1/15SP2 Operator Bundle for Kubernetes on Z
Fujitsu Enterprise Postgres Advanced Edition 15 Operator Bundle for Kubernetes on IBM Power(R)
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 15 for Kubernetes

Version 16:

Fujitsu Enterprise Postgres Advanced Edition 16/16SP1 for Linux
Fujitsu Enterprise Postgres Advanced Edition 16/16SP1 for Windows
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 16 for Linux
Fujitsu Enterprise Postgres Advanced Edition 16/16SP1 for Linux on Z
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 16 for Linux on Z
Fujitsu Enterprise Postgres Advanced Edition 16/16SP1 for Linux on IBM Power(R)
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 16 for Linux on IBM Power(R)
Fujitsu Enterprise Postgres Standard Edition 16/16SP1 for Linux
Fujitsu Enterprise Postgres Standard Edition 16/16SP1 for Windows
Fujitsu Enterprise Postgres Advanced Edition 16/16SP1 Operator Bundle for Kubernetes
Fujitsu Enterprise Postgres Advanced Edition 16/16SP1 Operator Bundle for Kubernetes on Z
Fujitsu Enterprise Postgres Advanced Edition 16/16SP1 Operator Bundle for Kubernetes on IBM Power(R)
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 16 for Kubernetes

Version 17:

Fujitsu Enterprise Postgres Advanced Edition 17/17SP1/17SP2 for Linux
Fujitsu Enterprise Postgres Advanced Edition 17/17SP1/17SP2 for Windows
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 17 for Linux
Fujitsu Enterprise Postgres Advanced Edition 17/17SP1 for Linux on Z
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 17 for Linux on Z

Fujitsu Enterprise Postgres Advanced Edition 17/17SP1 for Linux on IBM Power(R)

Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 17 for Linux on IBM Power(R)

Fujitsu Enterprise Postgres Standard Edition 17/17SP1/17SP2 for Linux

Fujitsu Enterprise Postgres Standard Edition 17/17SP1/17SP2 for Windows

Fujitsu Enterprise Postgres Advanced Edition 17/17SP1/17SP2 Operator Bundle for Kubernetes

Fujitsu Enterprise Postgres Advanced Edition 17/17SP1 Operator Bundle for Kubernetes on Z

Fujitsu Enterprise Postgres Advanced Edition 17/17SP1 Operator Bundle for Kubernetes on IBM Power(R)

Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 17 for Kubernetes

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	[x] Incident [] Application recommended	[] Degradation (EVL-UP)	[] Cautions
Impact on operation	The server is attacked by arbitrary code execution.		
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]

Manipulated input may cause arbitrary code execution when using selectivity estimation function.

[Environment]

- Linux
- Windows

[Conditions]

1) Selectivity estimation function is defined for the operator. AND

2) Manipulated SQL using the operator in 1) is executed.

 © Fujitsu 2026

2. Cause

There were issues in checking the type of the input in selectivity estimation function.

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]

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.