Fujitsu Enterprise Postgres

Urgent notification

Global Support News and IMPORTANT update information - No. GSI26-H036-01

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability CVE-2026-14678 reported by OSS PostgreSQL community.

Fujitsu Limited

Aug 17, 2026

Incident Information

[Incident management number] PH25525, PH25526, PH25527, PH25528, PH25529

- Description:

  The GiST picksplit function in contrib/pg_trgm may cause a buffer over-read.

  This is CVE-2026-14678 vulnerability reported by PostgreSQL community.

- Products and versions affected:

  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 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 2026

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 18/18SP1/18SP2 for Linux

Fujitsu Enterprise Postgres Advanced Edition 18/18SP1/18SP2 for Windows

Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 18 for Linux

Fujitsu Enterprise Postgres Standard Edition 18/18SP1/18SP2 for Linux

Fujitsu Enterprise Postgres Standard Edition 18/18SP1/18SP2 for Windows

Fujitsu Enterprise Postgres Advanced Edition 18/18SP1/18SP2 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	An incorrect GiST split decision may occur, or the server may crash.		
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]

   The GiST picksplit function in contrib/pg_trgm may cause a buffer over-read.

   [Environment]

   - Linux
   - Windows

   [Conditions]

   1) An operation is performed on an index using the pg_trgm GiST operator class.

2. Cause

   A data type error in the GiST picksplit function could read memory beyond the end of a buffer.

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 when the patch is made available.

   [Workaround]

   None.

 © Fujitsu 2026

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.