Fujitsu Enterprise Postgres

Urgent notification

Global Support News and IMPORTANT update information - No. GSI25-H007-01

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability CVE-2025-12818 reported by OSS PostgreSQL community.

Fujitsu Limited

Nov 14, 2025

Incident Information

[Incident management number] PH24958, PH24959, PH24960, PH24961, PH24962

- Description:

  Several functions could overflow their size calculations, when presented with very large inputs from remote and/or untrusted locations, and then allocate buffers that were too small to hold the intended contents.

  This is CVE-2025-12818 vulnerability reported by PostgreSQL community.

- Products and versions affected:

  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 Advanced Edition 13 for Linux on Z

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

  FUJITSU Enterprise Postgres Standard Edition 13 for Windows

  FUJITSU Enterprise Postgres Advanced Edition 13 Operator Bundle for Kubernetes

  FUJITSU Enterprise Postgres Advanced Edition 13 Operator Bundle for Kubernetes on Z

  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 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

Report classification	[x] Incident [] Degradation (EVL-UP) [] Cautions [] Application recommended
Impact on operation	Size calculations may cause overflow, potentially allocating a buffer that is too small to hold the intended content.
Recovery tasks	[] Required [x] Not required
Occurrence frequency	[x] Always [] Rarely [] Random [] Other ()
Workaround	[] Yes [x] No

Detailed Information

1. Issue and conditions to reproduce issue

[Issue]

Several functions could overflow their size calculations, when presented with very large inputs from remote and/or untrusted locations, and then allocate buffers that were too small to hold the intended contents.

[Environment]

- Linux
- Windows

[Conditions]

1) When very large inputs are provided to libpq functions.

2. Cause

There were issues allocating buffers that were too small to hold the intended contents.

3. How to avoid the issue

Apply patch when released by Fujitsu.
A community patch (for version 13-17) will be released soon, and a corresponding Fujitsu Enterprise Postgres patch (for version 13-17) 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]
First edition