Fujitsu Enterprise Postgres

Urgent notification

Global Support News and IMPORTANT update information - No. GSI25-H001-01

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability CVE-2025-1094 reported by OSS PostgreSQL community.

Fujitsu Limited

Feb 19, 2025

Incident Information

[Incident management number] PH24401, PH24402, PH24403, PH24404, PH24405

- Description:

  Malformed input can lead to SQL-injection attacks.

  This is CVE-2025-1094 vulnerability reported by PostgreSQL community.

- Products and versions affected:

  Version 9.5:

  FUJITSU Enterprise Postgres Advanced Edition 9.5/9.5SP1 for Linux

  FUJITSU Enterprise Postgres Advanced Edition 9.5/9.5SP1 for Windows

  FUJITSU Enterprise Postgres Standard Edition 9.5/9.5SP1 for Linux

  FUJITSU Enterprise Postgres Standard Edition 9.5/9.5SP1 for Windows

  Version 9.6:

  FUJITSU Enterprise Postgres Standard Edition 9.6 for Linux

  FUJITSU Enterprise Postgres Standard Edition 9.6 for Windows

  FUJITSU Enterprise Postgres Standard Edition 9.6 for Solaris

  Version 10:

  FUJITSU Enterprise Postgres Advanced Edition 10/10A for Linux

  FUJITSU Enterprise Postgres Advanced Edition 10/10A for Windows

  FUJITSU Enterprise Postgres Standard Edition 10/10A for Linux

  FUJITSU Enterprise Postgres Standard Edition 10/10A for Windows

Version 11:

FUJITSU Enterprise Postgres Advanced Edition 11 for Linux
FUJITSU Enterprise Postgres Advanced Edition 11 for Windows
FUJITSU Enterprise Postgres Standard Edition 11 for Linux
FUJITSU Enterprise Postgres Standard Edition 11 for Windows
FUJITSU Enterprise Postgres Advanced Edition 11 for Linux on Z

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 Advanced Edition 12/12SP1 for Linux on Z
FUJITSU Enterprise Postgres Standard Edition 12/12SP1/12SP1A/12SP1B for Linux
FUJITSU Enterprise Postgres Standard Edition 12/12SP1/12SP1A/12SP1B for Windows
FUJITSU Enterprise Postgres Advanced Edition 12/12SP1 Operator Bundle for Kubernetes
FUJITSU Enterprise Postgres Advanced Edition 12/12SP1 Operator Bundle for Kubernetes on Z

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 for Linux
Fujitsu Enterprise Postgres Advanced Edition 17 for Windows
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 17 for Linux
Fujitsu Enterprise Postgres Advanced Edition 17 for Linux on Z
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 17 for Linux on Z
Fujitsu Enterprise Postgres Advanced Edition 17 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 for Linux
Fujitsu Enterprise Postgres Standard Edition 17 for Windows
Fujitsu Enterprise Postgres Advanced Edition 17 Operator Bundle for Kubernetes
Fujitsu Enterprise Postgres Advanced Edition 17 Operator Bundle for Kubernetes on Z
Fujitsu Enterprise Postgres Advanced Edition 17 Operator Bundle for Kubernetes on IBM Power(R)
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module 17 for Kubernetes

Report classification	[x] Incident [] Application recommended	[] Degradation (EVL-UP)	[] Cautions
Impact on operation	The server is attacked by SQL-injection attacks.		
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]

   Malformed input can lead to SQL-injection attacks

   Improper neutralization of quoting syntax in PostgreSQL libpq functions allows a database input provider to achieve SQL injection in certain usage patterns. Specifically, SQL injection requires the application to use the function result to construct input to psql, the PostgreSQL interactive terminal.

   Similarly, improper neutralization of quoting syntax in PostgreSQL command line utility programs allows a source of command line arguments to achieve SQL injection
   when client_encoding is BIG5 and server_encoding is one of EUC_TW or MULE_INTERNAL

   [Environment]

   - Linux
   - Windows
   - Solaris

   [Conditions]

   1) Use one of the following libpq functions. AND
      - PQescapeLiteral()
      - PQescapeIdentifier()
      - PQescapeString()
      - PQescapeStringConn()
   2) The resulting string of the function 1) is passed through psql or other client commands.

2. Cause

   There were issues with libpq functions.

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 9.5-17) 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]
Third edition