

Fujitsu Enterprise Postgres

Urgent notification

Global Support News and IMPORTANT update information - No. GSI26-H017-01

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability [CVE-2026-54291](#) reported by PostgreSQL JDBC Driver community.

Fujitsu Limited

July 15, 2026

Incident Information

[Incident management number] PH25478

- Description:

In the PostgreSQL JDBC Driver, for connections where `channelBinding=require` was specified, there was a possibility that the authentication method could be downgraded from SCRAM-SHA-256-PLUS with channel binding to standard SCRAM-SHA-256 without channel binding without the user's knowledge. As a result, there was a risk that the protection against man-in-the-middle attacks could be lost.

This is CVE-2026-54291 vulnerability reported by PostgreSQL JDBC Driver community.

- Products and versions affected:

Version 16:

Fujitsu Enterprise Postgres Community Edition Client 16 for Linux

Fujitsu Enterprise Postgres Community Edition Client 16 for Windows

Fujitsu Enterprise Postgres Client 16/16SP1 for Linux

Fujitsu Enterprise Postgres Client 16/16SP1 for Windows

Fujitsu Enterprise Postgres Client with Cryptographic Module 16 for Linux

Fujitsu Enterprise Postgres Client with Cryptographic Module 16 for Windows

Version 17:

Fujitsu Enterprise Postgres Community Edition Client 17 for Linux

Fujitsu Enterprise Postgres Community Edition Client 17 for Windows

Fujitsu Enterprise Postgres Client 17/17SP1/17SP2 for Linux

Fujitsu Enterprise Postgres Client 17/17SP1/17SP2 for Windows

Fujitsu Enterprise Postgres Client with Cryptographic Module 17 for Linux

Version 18:

Fujitsu Enterprise Postgres Community Edition Client 18 for Linux

Fujitsu Enterprise Postgres Community Edition Client 18 for Windows

Fujitsu Enterprise Postgres Client 18/18SP1/18SP2 for Linux

Fujitsu Enterprise Postgres Client 18/18SP1/18SP2 for Windows

Fujitsu Enterprise Postgres Client with Cryptographic Module 18 for Linux

Fujitsu Enterprise Postgres Client with Cryptographic Module 18 for Windows

Report classification	☒ Incident	☐ Degradation (EVL-UP)	☐ Cautions
	☐ Application recommended		
Impact on operation	Silent channel binding authentication downgrade via unsupported certificate algorithms.		
Recovery tasks	☐ Required	☒ Not required	
Occurrence frequency	☒ Always	☐ Rarely	☐ Random
	☐ Other ()		
Workaround	☐ Yes	☒ No	

Detailed Information

1. Issue and conditions to reproduce issue

[Issue]

In the PostgreSQL JDBC Driver, for connections where `channelBinding=require` was specified, there was a possibility that the authentication method could be downgraded from SCRAM-SHA-256-PLUS with channel binding to standard SCRAM-SHA-256 without channel binding without the user's knowledge. As a result, there was a risk that the protection against man-in-the-middle attacks could be lost.

[Environment]

- Linux
- Windows

[Conditions]

- 1) If you are using an application that uses the PostgreSQL JDBC Driver. AND
- 2) When `channelBinding=require` is specified in the connection options.

2. Cause

There were issues in PostgreSQL JDBC Driver channel binding enforcement.

3. How to avoid the issue

Apply patch when released by Fujitsu.

A community patch has been released, and a corresponding Fujitsu Enterprise Postgres patch (for version 16-18) 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]

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.