Global Support News – GSI26-H062-01
Security Information

October, 26th, 2026

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability CVE-2026-107315 reported by OSS pgJDBC community.

Title: Enterprise Postgres: Data leakage vulnerability caused by crafted data transmission in pgJDBC

1. Description

In pgJDBC, when the data which is shorter than the declared length by an application was sent, residual data from a previously sent message could be included, potentially resulting in information disclosure.

Fujitsu provides security patches shown in 3.
Please apply them as soon as possible.

2. Impact

Under the following conditions, previously sent data may be included into stored data, potentially resulting in information disclosure.

1) An application sends data shorter than the declared length. AND
2) An attacker reads the affected data.

For a severity assessment of this vulnerability, see CVE information in "4. Related information".

3. Affected systems and corresponding action

3-1. Affected systems: PRIMERGY, GP5000, PRIMEQUEST

3-2. Affected products and required patch

Products	VL	Target OS	Package name	Patch ID for UpdateSite*1*2	Patch ID for RPM or MSI*1*3
Fujitsu Enterprise Postgres Community Edition Client	16	Linux		TBD	TBD
Fujitsu Enterprise Postgres Community Edition Client	16	Windows		TBD	TBD
Fujitsu Enterprise Postgres Client	16/16SP1	Linux		TBD	TBD
Fujitsu Enterprise Postgres Client	16/16SP1	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Client	16/16SP1	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Client	16/16SP1	Windows		TBD	TBD

 © Fujitsu 2026

Products	VL	Target OS	Package name	Patch ID for UpdateSite*1*2	Patch ID for RPM or MSI*1*3
Fujitsu Enterprise Postgres Client with Cryptographic Module	16	Linux		TBD	TBD
Fujitsu Enterprise Postgres Client with Cryptographic Module	16	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Client with Cryptographic Module	16	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Client with Cryptographic Module	16	Windows		TBD	TBD
Fujitsu Enterprise Postgres Community Edition Client	17	Linux		TBD	TBD
Fujitsu Enterprise Postgres Community Edition Client	17	Windows		TBD	TBD
Fujitsu Enterprise Postgres Client	17/17SP1/17SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Client	17/17SP1/17SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Client	17/17SP1/17SP2	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Client	17/17SP1/17SP2	Windows		TBD	TBD
Fujitsu Enterprise Postgres Client with Cryptographic Module	17	Linux		TBD	TBD
Fujitsu Enterprise Postgres Client with Cryptographic Module	17	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Client with Cryptographic Module	17	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Client with Cryptographic Module	17	Windows		TBD	TBD
Fujitsu Enterprise Postgres Community Edition Client	18	Linux		TBD	TBD
Fujitsu Enterprise Postgres Community Edition Client	18	Windows		TBD	TBD
Fujitsu Enterprise Postgres Client	18/18SP1/18SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Client	18/18SP1/18SP2	Windows		TBD	TBD
Fujitsu Enterprise Postgres Client with Cryptographic Module	18	Linux		TBD	TBD
Fujitsu Enterprise Postgres Client with Cryptographic Module	18	Windows		TBD	TBD

[*1] Patches may be provided in different package formats (such as UpdateSite, RPM, or MSI). Please refer to the applicable package for your environment.
[*2] For information on how to obtain UpdateSite format patches, please contact your local representative at Fujitsu Limited.
[*3] Please obtain RPM or MSI format patches from JFrog.

3-3. Workaround

None.

Note that the workarounds cannot completely solve this problem. For this reason, apply the relevant patch as soon as it is released.

 © Fujitsu 2026

4. Related information

CVE-2026-107315
"Data leakage vulnerability caused by crafted data transmission in pgJDBC"
- CVE: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2026-107315

Fujitsu Technical Support resources
https://www.postgresql.fastware.com/fujitsu-support-engineering

5. Revision history

October 26th, 2026: Initial release

This bulletin provides security information about the reports to Japan Computer Emergency Response Team Coordination Center(JPCERT/CC), the coordination center, or detected by Fujitsu's own examination by the published date.

Products developed by third parties may be included as subject products. Information about such third party products may be exactly the same as provided by the respective third party.

The contents of this bulletin are provided "AS IS" without warranties of any kind, either express or implied (including, without limitation, any implied warranty of merchantability, fitness for a particular purpose and non-infringement). In no event shall Fujitsu be liable for any direct, indirect, special, incidental, consequential, punitive, or any other damages of any kind, including, without limitation, loss of profits and loss of data incurred by a customer arising out of, or in connection with, the use or non-use of any information in this bulletin, even if Fujitsu has been advised of the possibility of such damages.

The information contained in this bulletin will be updated from time to time without notice. Therefore, all customers are advised to always ascertain the latest information. In case of redistribution of this security bulletin, the full text of this statement shall be reproduced.

© 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.