Global Support News – GSI26-H065-01
Security Information

November, 6th, 2026

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability CVE-2026-116252 reported by OSS pgAdmin4 community.

Title: Enterprise Postgres: Information disclosure vulnerability due to connection redirection in updating materialized views in pgAdmin4

1. Description

When updating a materialized view in pgAdmin4, the target database name could potentially be interpreted as connection information.
Due to this issue, if a role with only the CREATEDB privilege created a database with a crafted name, an attacker could change the psql connection target to a server of their choice, potentially leading to the disclosure of the connected user's stored password.

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

2. Impact

Under the following conditions, the connection may be changed to a server specified by the attacker, potentially resulting in the disclosure of authentication information such as stored passwords.

1) An attacker with the CREATEDB privilege creates a database with a name that includes connection information. AND
2) Materialized view for that database is updated by pgAdmin4.

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 Client	14/14A/ 14SP1	Windows		TBD	TBD
Fujitsu Enterprise Postgres Client	15/15SP1/ 15SP2	Windows		TBD	TBD
Fujitsu Enterprise Postgres Client	16/16SP1	Windows		TBD	TBD
Fujitsu Enterprise Postgres Client	17/17SP1/ 17SP2	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	18/18SP1/ 18SP2	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.

4. Related information

CVE-2026-116252
"Information disclosure vulnerability due to connection redirection in updating materialized views in pgAdmin4"
- CVE: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2026-116252

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

5. Revision history

November 6th, 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.