Global Support News – GSI26-H066-01
Security Information

November, 5th, 2026

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability CVE-2026-111497 reported by Google.

Title: Enterprise Postgres: Vulnerabilities in the Brotli module, including memory corruption, information disclosure, denial of service, and arbitrary code execution due to out-of-bounds writes

1. Description

When using the Deploy Cloud Instance feature in pgAdmin4, if a network attacker has tampered with the response from the target web service, a vulnerability in the bundled Brotli module could lead to memory corruption, information disclosure, denial of service, or arbitrary code execution.

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

2. Impact

Under the following conditions, decompressing a malformed Brotli compression stream could result in memory corruption, information disclosure, a denial of service, or arbitrary code execution.

1) Responses from external services accessed via the Deploy Cloud Instance feature of pgAdmin4 have been tampered with by a network attacker. AND
2) An instance has been deployed to a database service provided by any cloud provider using the Deploy Cloud Instance feature of 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	12	Windows		TBD	TBD
FUJITSU Enterprise Postgres Client	12SP1/12SP1A/ 12SP1B	Windows		TBD	TBD
FUJITSU Enterprise Postgres Client	13	Windows		TBD	TBD
FUJITSU Enterprise Postgres Client	13SP1/13SP1A/	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	14/14SP1	Windows		T016859XP-21	FJSVfsep-ADMIN4-1401-21.msi
Fujitsu Enterprise Postgres Client	15/15SP1/ 15SP2	Windows		T017201XP-19	FJSVfsep-ADMIN4-1502-17.msi
Fujitsu Enterprise Postgres Client	16/16SP1	Windows		T017634XP-15	FJSVfsep-ADMIN4-1601-14.msi
Fujitsu Enterprise Postgres Client	17/17SP1/ 17SP2	Windows		T017852XP-13	FJSVfsep-ADMIN4-1702-10.msi
Fujitsu Enterprise Postgres Client	18/18SP1/ 18SP2	Windows		T018128XP-08	FJSVfsep-client-pgadmin4-1802-6.msi

[*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-2026-111497
"A buffer overflow vulnerability in the Brotli decoder (c/dec/decode.c) in Google Brotli versions 1.0.3 through 1.2.0 on all platforms allows a remote unauthenticated attacker to corrupt adjacent decoder state memory, disclose sensitive memory contents, cause a denial of service, or potentially execute arbitrary code using a crafted Brotli-compressed stream."
- CVE: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2026-111497

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

 © Fujitsu 2026

5. Revision history

November 5th, 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.