Global Support News – GSI26-H074-01
Security Information

November, 16th, 2026

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability CVE-2026-116304 reported by OSS PostgreSQL community.

Title: Enterprise Postgres: Use-after-free in shared tuple descriptor management

---

1. Description

A race condition in shared tuple descriptor management could result in use of freed memory.

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

2. Impact

If shared tuple descriptor management operations race, freed memory may be used, potentially causing abnormal server termination or memory corruption.

For a severity assessment of this vulnerability, see JVN 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 Advanced Edition	14/14SP1	Linux		TBD	TBD
FUJITSU Enterprise	14/14SP1	Windows		TBD	TBD

 © Fujitsu 2026

Postgres Advanced Edition				
FUJITSU Enterprise Postgres Community Edition	14	Linux	TBD	TBD
FUJITSU Enterprise Postgres Community Edition	14	Windows	TBD	TBD
FUJITSU Enterprise Postgres Standard Edition	14	Linux	TBD	TBD
FUJITSU Enterprise Postgres Standard Edition	14	Windows	TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	15/15SP1/15SP2	Linux	TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	15/15SP1/15SP2	Windows	TBD	TBD
Fujitsu Enterprise Postgres Community Edition	15	Linux	TBD	TBD
Fujitsu Enterprise Postgres Community Edition	15	Windows	TBD	TBD
Fujitsu Enterprise Postgres Standard Edition	15/15SP1/15SP2	Linux	TBD	TBD
Fujitsu Enterprise Postgres Standard Edition	15/15SP1/15SP2	Windows	TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	16/16SP1	Linux	TBD	TBD

 © Fujitsu 2026

Fujitsu Enterprise Postgres Advanced Edition	16/16SP1	Windows	TBD	TBD
Fujitsu Enterprise Postgres Community Edition	16	Linux	TBD	TBD
Fujitsu Enterprise Postgres Community Edition	16	Windows	TBD	TBD
Fujitsu Enterprise Postgres Standard Edition	16/16SP1	Linux	TBD	TBD
Fujitsu Enterprise Postgres Standard Edition	16/16SP1	Windows	TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	17/17SP1/17SP2	Linux	TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	17/17SP1/17SP2	Windows	TBD	TBD
Fujitsu Enterprise Postgres Community Edition	17	Linux	TBD	TBD
Fujitsu Enterprise Postgres Community Edition	17	Windows	TBD	TBD
Fujitsu Enterprise Postgres Standard Edition	17/17SP1/17SP2	Linux	TBD	TBD
Fujitsu Enterprise Postgres Standard Edition	17/17SP1/17SP2	Windows	TBD	TBD
Fujitsu Enterprise Postgres	18/18SP1/18SP2	Linux	TBD	TBD

 © Fujitsu 2026

Advanced Edition				
Fujitsu Enterprise Postgres Advanced Edition	18/18SP1/18SP2	Windows	TBD	TBD
Fujitsu Enterprise Postgres Community Edition	18	Linux	TBD	TBD
Fujitsu Enterprise Postgres Community Edition	18	Windows	TBD	TBD
Fujitsu Enterprise Postgres Standard Edition	18/18SP1/18SP2	Linux	TBD	TBD
Fujitsu Enterprise Postgres Standard Edition	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-2026-116304
"Use-after-free in shared tuple descriptor management"
- CVE: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2026-116304

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

5. Revision history

November 16th, 2026: Initial release

 © Fujitsu 2026

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.