

Global Support News – GSI26-H059-01

Security Information



October, 9th, 2026

This is to inform you of the impact on Fujitsu Enterprise Postgres of the recent security vulnerability CVE-2026-54872 reported by OSS OpenSSL community.

Title: Enterprise Postgres: Vulnerability in OpenSSL allowing private key guessing due to the use of ECDSA certificates based on non-NIST elliptic curve

1. Description

If a user was using an ECDSA certificate based on a non-NIST elliptic curve, there was a risk that the private key could be guessed.

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

2. Impact

Under the following conditions, the private key may be guessed, resulting in information disclosure.

- 1) An ECDSA certificate with a non-NIST elliptic curve is used. AND
- 2) An attacker observes the signing time many times.

The following OSS products are affected.

- PostgreSQL
- Pgpool-II
- pgBackRest
- psqlODBC

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 Postgres Advanced Edition	14/14SP1	Linux on Z		TBD	TBD
FUJITSU Enterprise Postgres Advanced Edition	14/14SP1	Linux on IBM Power(R)		TBD	TBD
FUJITSU Enterprise Postgres Advanced Edition	14/14SP1	Windows		TBD	TBD

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	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 for Kubernetes	14/14SP1	Linux		TBD	TBD
FUJITSU Enterprise Postgres Advanced Edition for Kubernetes	14/14SP1	Linux on Z		TBD	TBD
FUJITSU Enterprise Postgres Advanced Edition for Kubernetes	14/14SP1	Linux on IBM Power(R)		TBD	TBD
FUJITSU Enterprise Postgres Community Edition Client	14	Linux		TBD	TBD
FUJITSU Enterprise Postgres Community Edition Client	14	Windows		TBD	TBD
FUJITSU Enterprise Postgres Client	14/14SP1	Linux		TBD	TBD
FUJITSU Enterprise Postgres Client	14/14SP1	Linux on Z		TBD	TBD
FUJITSU Enterprise Postgres Client	14/14SP1	Linux on IBM Power(R)		TBD	TBD
FUJITSU Enterprise Postgres Client	14/14SP1	Windows		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	15/15SP1/15SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	15/15SP1/15SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	15/15SP1/15SP2	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	15/15SP1/15SP2	Windows		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module	15	Linux		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module	15	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module	15	Linux on IBM Power(R)		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

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 for Kubernetes	15/15SP1/15SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition for Kubernetes	15/15SP1/15SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition for Kubernetes	15/15SP1/15SP2	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module for Kubernetes	15	Linux		TBD	TBD
Fujitsu Enterprise Postgres Community Edition Client	15	Linux		TBD	TBD
Fujitsu Enterprise Postgres Community Edition Client	15	Windows		TBD	TBD
Fujitsu Enterprise Postgres Client	15/15SP1/15SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Client	15/15SP1/15SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Client	15/15SP1/15SP2	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Client	15/15SP1/15SP2	Windows		TBD	TBD
Fujitsu Enterprise Postgres Client with Cryptographic Module	15	Linux		TBD	TBD
Fujitsu Enterprise Postgres Client with Cryptographic Module	15	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Client with Cryptographic Module	15	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	16/16SP1	Linux		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	16/16SP1	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	16/16SP1	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	16/16SP1	Windows		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module	16	Linux		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module	16	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module	16	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Community Edition	16	Linux		TBD	TBD

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	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 for Kubernetes	16/16SP1	Linux		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition for Kubernetes	16/16SP1	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition for Kubernetes	16/16SP1	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module for Kubernetes	16	Linux		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module for Kubernetes	16	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module for Kubernetes	16	Linux on IBM Power(R)		TBD	TBD
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 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 Advanced Edition	17/17SP1/ 17SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	17/17SP1/ 17SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	17/17SP1/ 17SP2	Linux on IBM Power(R)		TBD	TBD

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	17/17SP1/ 17SP2	Windows		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module	17	Linux		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module	17	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module	17	Linux on IBM Power(R)		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 Advanced Edition for Kubernetes	17/17SP1/ 17SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition for Kubernetes	17/17SP1/ 17SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition for Kubernetes	17/17SP1/ 17SP2	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module for Kubernetes	17	Linux		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

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	18/18SP1/18SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition	18/18SP1/18SP2	Windows		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module	18	Linux		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
Fujitsu Enterprise Postgres Advanced Edition for Kubernetes	18/18SP1/18SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Advanced Edition with Cryptographic Module for Kubernetes	18	Linux		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
FUJITSU Enterprise Postgres Pgpool-II	14/14SP1	Linux		TBD	TBD
FUJITSU Enterprise Postgres Pgpool-II	14/14SP1	Linux on Z		TBD	TBD
FUJITSU Enterprise Postgres Pgpool-II	14/14SP1	Linux on IBM Power(R)		TBD	TBD
FUJITSU Enterprise Postgres Pgpool-II for Kubernetes	14/14SP1	Linux		TBD	TBD
FUJITSU Enterprise Postgres Pgpool-II for Kubernetes	14/14SP1	Linux on Z		TBD	TBD
FUJITSU Enterprise Postgres Pgpool-II for Kubernetes	14/14SP1	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II	15/15SP1/15SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II	15/15SP1/15SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II	15/15SP1/15SP2	Linux on IBM Power(R)		TBD	TBD

Products	VL	Target OS	Package name	Patch ID for UpdateSite ^{*1-2}	Patch ID for RPM or MSI ^{*1-3}
Fujitsu Enterprise Postgres Pgpool-II for Kubernetes	15/15SP1/15SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II for Kubernetes	15/15SP1/15SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II for Kubernetes	15/15SP1/15SP2	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II	16/16SP1	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II	16/16SP1	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II	16/16SP1	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II for Kubernetes	16/16SP1	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II for Kubernetes	16/16SP1	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II for Kubernetes	16/16SP1	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II	17/17SP1/17SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II	17/17SP1/17SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II	17/17SP1/17SP2	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II for Kubernetes	17/17SP1/17SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II for Kubernetes	17/17SP1/17SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II for Kubernetes	17/17SP1/17SP2	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II	18/18SP1/18SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II for Kubernetes	18/18SP1/18SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module	15	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module	15	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module	15	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module for Kubernetes	15	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module for Kubernetes	15	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module for Kubernetes	15	Linux on IBM Power(R)		TBD	TBD

Products	VL	Target OS	Package name	Patch ID for UpdateSite ^{*1-2}	Patch ID for RPM or MSI ^{*1-3}
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module	16	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module	16	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module	16	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module for Kubernetes	16	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module for Kubernetes	16	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module for Kubernetes	16	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module	17	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module	17	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module	17	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module for Kubernetes	17	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module for Kubernetes	17	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module for Kubernetes	17	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module	18	Linux		TBD	TBD
Fujitsu Enterprise Postgres Pgpool-II with Cryptographic Module for Kubernetes	18	Linux		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest	15SP1/ 15SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest	15SP1/ 15SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest	15SP1/ 15SP2	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest for Kubernetes	15SP1/ 15SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest for Kubernetes	15SP1/ 15SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest for Kubernetes	15SP1/ 15SP2	Linux on IBM Power(R)		TBD	TBD

Products	VL	Target OS	Package name	Patch ID for UpdateSite ^{*1-2}	Patch ID for RPM or MSI ^{*1-3}
Fujitsu Enterprise Postgres pgBackRest	16/16SP1	Linux		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest	16/16SP1	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest	16/16SP1	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest for Kubernetes	16/16SP1	Linux		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest for Kubernetes	16/16SP1	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest for Kubernetes	16/16SP1	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest	17/17SP1/ 17SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest	17/17SP1/ 17SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest	17/17SP1/ 17SP2	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest for Kubernetes	17/17SP1/ 17SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest for Kubernetes	17/17SP1/ 17SP2	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest for Kubernetes	17/17SP1/ 17SP2	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest	18/18SP1/ 18SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest for Kubernetes	18/18SP1/ 18SP2	Linux		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module	16	Linux		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module	16	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module	16	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module for Kubernetes	16	Linux		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module for Kubernetes	16	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module for Kubernetes	16	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module	17	Linux		TBD	TBD

Products	VL	Target OS	Package name	Patch ID for UpdateSite ^{*1-2}	Patch ID for RPM or MSI ^{*1-3}
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module	17	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module	17	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module for Kubernetes	17	Linux		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module for Kubernetes	17	Linux on Z		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module for Kubernetes	17	Linux on IBM Power(R)		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module	18	Linux		TBD	TBD
Fujitsu Enterprise Postgres pgBackRest with Cryptographic Module for Kubernetes	18	Linux		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-2026-54872

"Vulnerability in OpenSSL allowing private key guessing due to the use of ECDSA certificates based on non-NIST elliptic curve"

- CVE: <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2026-54872>

Fujitsu Technical Support resources

<https://www.postgresql.fastware.com/fujitsu-support-engineering>

5. Revision history

October 9th, 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.