

Urgent notification

Global Support News and IMPORTANT update information - No. GSI23-H001-01

Fujitsu Limited is notifying of an issue with FUJITSU Enterprise Postgres (FEP).

Fujitsu Limited

Dec 25, 2023

Incident Information

[Incident management number] None.

- Description:
 - FEP products are not impacted by the CVE-2023-50164 vulnerability, as Apache Struts2 is not bundled with them.
- Product name:
 - Fujitsu Enterprise Postgres
 - 15 (Windows64-EM64T)
 - 15 – 15SP1 (Linux64-EM64T)
 - Fujitsu Enterprise Postgres Client
 - 15 (Windows32, Windows64-EM64T, Linux64-EM64T)
 - Fujitsu Enterprise Postgres Community Edition Client
 - 15 (Windows32, Windows64-EM64T, Linux64-EM64T)

 - FUJITSU Enterprise Postgres
 - 14 (Windows64-EM64T)
 - 14 - 14SP1 (Linux64-EM64T)
 - FUJITSU Enterprise Postgres Client
 - 14 - 14A (Windows32, Windows64-EM64T, Linux64-EM64T)
 - FUJITSU Enterprise Postgres Community Edition Client
 - 14 (Windows32, Windows64-EM64T, Linux64-EM64T)

 - FUJITSU Enterprise Postgres
 - 13 - 13SP1A (Windows64-EM64T, Linux64-EM64T)

FUJITSU Enterprise Postgres Client

13 - 13SP1A (Windows32, Windows64-EM64T, Linux64-EM64T)

FUJITSU Enterprise Postgres Community Edition Client

13 - 13SP1A (Windows32, Windows64-EM64T, Linux64-EM64T)

FUJITSU Enterprise Postgres

12 - 12SP1B (Windows64-EM64T, Linux64-EM64T)

FUJITSU Enterprise Postgres Advanced Edition (without encryption)

12 - 12SP1 (Windows64-EM64T)

12 (Linux64-EM64T)

FUJITSU Enterprise Postgres Client

12 - 12SP1B (Windows32, Windows64-EM64T, Linux64-EM64T)

FUJITSU Enterprise Postgres Client (without encryption)

12 - 12SP1 (Windows32, Windows64-EM64T, Linux64-EM64T)

FUJITSU Enterprise Postgres Community Edition Client

12 - 12SP1A (Windows32, Windows64-EM64T, Linux64-EM64T)

FUJITSU Enterprise Postgres Standard Edition (without encryption)

12 - 12SP1 (Windows64-EM64T)

12 (Linux64-EM64T)

FUJITSU Enterprise Postgres

11 (Windows64-EM64T, Linux64-EM64T)

FUJITSU Enterprise Postgres Client

11 (Windows32, Windows64-EM64T, Linux32, Linux64-EM64T)

FUJITSU Enterprise Postgres Community Edition Client

11 (Windows32, Windows64-EM64T, Linux32, Linux64-EM64T)

FUJITSU Enterprise Postgres

10 - 10A (Windows64-EM64T, Linux64-EM64T)

FUJITSU Enterprise Postgres Client

10 - 10A (Windows32, Windows64-EM64T, Linux32, Linux64-EM64T)

FUJITSU Enterprise Postgres Community Edition Client

10 - 10A (Windows32, Windows64-EM64T, Linux32, Linux64-EM64T)

FUJITSU Enterprise Postgres

9.6 (Windows64-EM64T, Linux64-EM64T, Solaris)

FUJITSU Enterprise Postgres Client

9.6 - 9.6A (Windows32, Windows64-EM64T, Linux32, Linux64-EM64T)

FUJITSU Enterprise Postgres Client (32bit)

9.6 - 9.6A (Solaris)

FUJITSU Enterprise Postgres Client (64bit)

9.6 - 9.6A (Solaris)

FUJITSU Enterprise Postgres

9.5 - 9.5A (Windows64-EM64T)

FUJITSU Enterprise Postgres Client

9.5 - 9.5D (Windows32, Windows64-EM64T, Linux32, Linux64-EM64T)

FUJITSU Enterprise Postgres (without encryption)

9.5 (Windows64-EM64T)

FUJITSU Enterprise Postgres Client (without encryption)

9.5 - 9.5A (Windows32, Windows64-EM64T, Linux32, Linux64-EM64T)

Report classification	<input checked="" type="checkbox"/> Incident <input type="checkbox"/> Application recommended	<input type="checkbox"/> Degradation (EVL-UP)	<input type="checkbox"/> Cautions
Impact on operation	No impact		
Recovery tasks	<input type="checkbox"/> Required	<input checked="" type="checkbox"/> Not required	
Occurrence frequency	<input type="checkbox"/> Always <input checked="" type="checkbox"/> Other (Does not occur)	<input type="checkbox"/> Rarely	<input type="checkbox"/> Random
Workaround	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No	

Detailed Information

1. Issue and conditions to reproduce issue

[Issue]

A vulnerability in Apache Struts2, CVE-2023-50164, has been reported. This vulnerability could potentially allow an attacker to manipulate the file upload parameter to enabling path traversal. Under certain circumstances, this could lead to the upload of a malicious file, which could be used to execute remote code.

[Environment]

- Linux
- Windows
- Solaris

[Conditions]

- 1) Install FUJITSU Enterprise Postgres.

2. Cause

A vulnerability in Apache Struts2, CVE-2023-50164, has been reported.

Apache Struts2 is not bundled with FEP products.

3. How to avoid the issue

None.

[Workaround]

None.

4. Recovery measures after the issue occurs

None.

5. Other

None.

[Revision history]

First edition

© Fujitsu 2023. 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.