

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. To learn more, view the following link: [Privacy Policy](#)



[Manage Preferences](#)

more [here](#).

CVE-2024-47552 PUBLISHED

[View JSO](#)

Required CVE Record Information

CNA: Apache Software Foundation

Published: 2025-03-20 **Updated:** 2026-03-30

Title: Apache Seata (incubating): Deserialization of untrusted Data in jraft mode in Apache Seata Server

Description

Deserialization of Untrusted Data vulnerability in Apache Seata (incubating). This issue affects Apache Seata (incubating) before 2.2.0. Severity Justification: The Apache Seata security team assesses the severity of this vulnerability as "Low" real-world mitigating factors. First, the vulnerability is strictly isolated to the Raft cluster mode, an optional and non-default mode introduced in v2.0.0, while most users rely on the unaffected traditional architecture. Second, Seata is an internal middle component for communication between TC and RM/TM occurs entirely within trusted internal networks. An attacker would require prior access to the Intranet to exploit this, making external exploitation highly improbable. Users are recommended to upgrade to version 2.2.0 which fixes the issue.

CWE 1 Total

[Learn more](#)

- [CWE-502: CWE-502 Deserialization of Untrusted Data](#)

Product Status

[Learn more](#)

Vendor	Product
Apache Software Foundation	Apache Seata (incubating)

Versions 1 Total

Default Status: unaffected

Affected

- affected from **2.0.0** before **2.2.0**

Credits

- liuhuajin<liuhuajin1@huawei.com> finder
- llqxc369@gmail.com finder

This website utilizes technologies such as cookies to enable essential site functionality, as well as for analytics, personalization, and targeted advertising. To learn more, view the following link: [Privacy Policy](#)

CVE Program

Updated: 2025-03-20

This container includes required additional information provided by the CVE Program for this vulnerability.

References 1 Total

- <http://www.openwall.com/lists/oss-security/2025/03/19/5>

Authorized Data Publishers

[Learn more](#)

CISA-ADP

Policies & Cookies

- [Terms of Use](#)
- [Website Security Policy](#)
- [Privacy Policy](#)
- [Cookie Notice](#)
- [Manage Cookies](#)

Media

- [News](#)
- [Blogs](#)
- [Podcasts](#)
- [Email newsletter sign up](#)

Social Media

- [!\[\]\(3dc92c626ede9fa1b47e2e010104b5c4_img.jpg\)](#)
- [!\[\]\(71e9a2c5583c3d2a2fe005f4239e5d39_img.jpg\)](#)
- [!\[\]\(5aa86d4510bccda8326cff2d2412c12b_img.jpg\)](#)
- [!\[\]\(1ed15c9cc7c61868b75e5155e86ba5c0_img.jpg\)](#)
- [!\[\]\(37547a2901c4baef73624871bb30efd8_img.jpg\)](#)
- [!\[\]\(4f868c32b7dc0803f13b34236fdbf50e_img.jpg\)](#)
- [New CVE Records](#)
- [CVE Announce](#)

Contact

- [CVE Program Support](#)
- [CNA Partners](#)
- [CVE Website Feedback Form](#)
- [CVE Website Support](#)

Use of the CVE™ List and the associated references from this website are subject to the [terms of use](#). CVE is sponsored by the [U.S. Department of Homeland Security \(DHS\)](#) [Cybersecurity and Infrastructure Security Agency \(CISA\)](#). Copyright © 1999-2026, [The MITRE Corporation](#). CVE is a trademark and the CVE logo is a registered trademark of The MITRE Corporation.

Links that redirect to external websites [↗](#) will open a new window or tab depending on the web browser used.