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 (incubatir 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-defa introduced in v2.0.0, while most users rely on the unaffected traditional architecture. Second, Seata is an internal middl communication between TC and RM/TM occurs entirely within trusted internal networks. An attacker would require prio access to the Intranet to exploit this, making external exploitation highly improbable. Users are recommended to upgra which fixes the issue.

CWE 1 Total

Learn more

- CWE-502: CWE-502 Deserialization of Untrusted Data

Product Status

Learn more

Vendor
Apache Software Foundation

Product
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

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.