

Log4J Vulnerability CVE-2026-49844

000045921 | How To | Last updated 2026-09-02 | Communications Manager

Issue

Log4J Vulnerability CVE-2026-49844 reported.

Improper encoding of non-finite floating-point values during MapMessage JSON serialization in Apache Log4j API produces output that is not valid JSON. This issue affects Apache Log4j API versions 2.13.1 through 2.25.4 and version 2.26.0.

Full details [NVD-CVE-2026-49844](#)

Cause

The fix for CVE-2026-34481 did not cover all code paths: when a MapMessage contains a non-finite IEEE 754 value (NaN, Infinity, or -Infinity), MapMessage.asJson() emits the corresponding bare token.

Full details [NVD-CVE-2026-49844](#)

Solution

- Upgrade log4j-api-2.25.4.jar to log4j-api-2.26.1.jar
- Upgrade log4j-core-2.25.4.jar to log4j-core-2.26.1.jar
- Upgrade log4j-slf4j-impl-2.25.4.jar to log4j-slf4j-impl-2.26.1.jar
- Upgrade log4j-web-2.25.4.jar to log4j-web-2.26.1.jar

Applies to

Product	Version	Build	Environment	Hardware
---------	---------	-------	-------------	----------

References

[NVD-CVE-2026-49844](#)

<https://aio-eus-uat-cae-aif-app14-local.redglacier-35d7ee4f.eastus.azurecontainerapps.io/article/45921>