CVE-2021-39194

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-39194
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-07 20:15:00 UTC
Updated	2021-09-14 17:06:00 UTC
Description	kaml is an open source implementation of the YAML format with support for kotlinx.serialization. In affected versions attacke

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kaml Project	Kaml	All	All	All	All

References

Reference	Source
Fix issue where decoding a polymorphic type that uses the tag polymor… · charleskorn/kaml@e18785d · GitHub	MISC
Polymorphic serialization hangs · Issue #179 · charleskorn/kaml · GitHub	MISC
Potential denial of service while parsing polymorphic input with tagged polymorphism style · Advisory · charleskorn/kaml · GitHub	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981155 Java (maven) Security Update for com.charleskorn.kaml:kaml (GHSA-fmm9-3gv8-58f4)

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report