



CVE-2023-28118

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-28118
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-20 13:15:00 UTC
Updated	2023-03-24 18:00:00 UTC
Description	kaml provides YAML support for kotlinx.serialization. Prior to version 0.53.0, applications that use kaml to parse untrusted in

Risk And Classification

Problem Types: CWE-776

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	Link	T
Default to not parsing anchors and aliases to prevent "billion laughs..." · charleskorn/kaml@5f82a2d · GitHub	MISC	github.com	
Potential denial of service while parsing input with anchors and aliases · Advisory · charleskorn/kaml · GitHub	MISC	github.com	
Release 0.53.0 · charleskorn/kaml · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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 registered 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