



CVE-2020-8570

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-8570
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-21 17:15:00 UTC
Updated	2023-11-07 03:26:00 UTC
Description	Kubernetes Java client libraries in version 10.0.0 and versions prior to 9.0.1 allow writes to paths outside of the current dire

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kubernetes	Java	All	All	All	All
Application	Kubernetes	Java	All	All	All	All

References

Reference	Source	Link
Pony Mail!	MLIST	lists.apache
Pony Mail!		lists.apache
Pony Mail!	MLIST	lists.apache
Fwd: [Security Advisory] CVE-2020-8570: Path Traversal bug in the Java Kubernetes Client	MLIST	groups.goo
Pony Mail!		lists.apache
Pony Mail!		lists.apache
CVE-2020-8570: Path Traversal bug in the Java Kubernetes Client · Issue #1491 · kubernetes-client/java · GitHub	CONFIRM	github.com
Pony Mail!	MLIST	lists.apache
Pony Mail!		lists.apache
Pony Mail!	MLIST	lists.apache
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Discovered via CodeQL automated scanning on GitHub

Legacy QID Mappings

982803 Java (maven) Security Update for io.kubernetes:client-java (GHSA-cghx-9gcr-r42x)

© [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 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)