



CVE-2022-21126

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

Summary

CVE	CVE-2022-21126
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-29 17:15:00 UTC
Updated	2022-12-01 21:08:00 UTC
Description	The package com.github.samtools:htsjdk before 3.0.1 are vulnerable to Creation of Temporary File in Directory with Insecure Permissions in com.github.samtools:htsjdk CVE-2022-21126 Snyk

Risk And Classification

Problem Types: CWE-668

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Samtools	Htsjdk	All	All	All	All

References

Reference
[SECURITY] Fix Temporary Directory Hijacking or Information Disclosure Vulnerability by JLLeitschuh · Pull Request #1617 · samtools/htsjdk
Fix temporary directory hijacking or temporary directory information ... · samtools/htsjdk@4a4024a · GitHub
Creation of Temporary File in Directory with Insecure Permissions in com.github.samtools:htsjdk CVE-2022-21126 Snyk
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit
LEGACY: Jonathan Leitschuh

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

© [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](#).

Free CVE JSON API [cve.report/api](#)

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