



CVE-2022-21230

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

Summary

CVE	CVE-2022-21230
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-01 16:15:00 UTC
Updated	2022-05-11 14:34:00 UTC
Description	This affects all versions of package org.nanohttpd:nanohttpd. Whenever an HTTP Session is parsing the body of an HTTP

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nanohttpd	Nanohttpd	All	All	All	All

References

Reference	Source
github.com/NanoHttpd/nanohttpd/blob/efb2ebf85a2b06f7c508aba9eaad5377e3a0...	MISC
Creation of Temporary File With Insecure Permissions in org.nanohttpd:nanohttpd · Advisory · JLLeitschuh/security-research · GitHub	MISC
github.com/NanoHttpd/nanohttpd/blob/efb2ebf85a2b06f7c508aba9eaad5377e3a0...	MISC
Information Exposure in org.nanohttpd:nanohttpd CVE-2022-21230 Snyk	MISC
nanohttpd/DefaultTempFile.java at efb2ebf85a2b06f7c508aba9eaad5377e3a01e81 · NanoHttpd/nanohttpd · GitHub	MITRE
nanohttpd/DefaultTempFileManager.java at efb2ebf85a2b06f7c508aba9eaad5377e3a01e81 · NanoHttpd/nanohttpd · GitHub	MITRE
CVE Program record	CVE
NVD vulnerability detail	NVD

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](#)