



CVE-2021-23520

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

Summary

CVE	CVE-2021-23520
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-31 11:15:00 UTC
Updated	2022-02-04 20:33:00 UTC
Description	The package juice-framework/juce before 6.1.5 are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip) via the

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
ZipFile: Add path checks to uncompressEntry() · juice-framework/JUCE@2e874e8 · GitHub	CONFIRM	github.com	
Arbitrary File Write via Archive Extraction (Zip Slip) in juice-framework/JUCE CVE-2021-23520 Snyk	CONFIRM	snyk.io	
Zip Slip Vulnerability Snyk	CONFIRM	snyk.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

Vendor Comments And Credit

Discovery Credit

LEGACY: Snyk Security Research Team

Legacy QID Mappings

[181989](#) Debian Security Update for juice (CVE-2021-23520)

© [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](#)