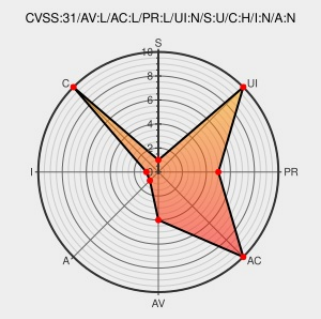
CVE-2021-23521

Published on: 01/31/2022 12:00:00 AM UTC

Last Modified on: 02/07/2022 06:32:00 PM UTC

CVE-2021-23521

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Juce from Juce contain the following vulnerability:

This affects the package juce-framework/JUCE before 6.1.5. This vulnerability is triggered when a malicious archive is crafted with an entry containing a symbolic link. When extracted, the symbolic link is followed outside of the target dir allowing writing arbitrary files on the target host. In some cases, this can allow an attacker to execute arbitrary code. The vulnerable code is in the ZipFile::uncompressEntry function in juce_ZipFile.cpp and is executed when the archive is extracted upon calling uncompressTo() on a ZipFile object.

CVE-2021-23521 has been assigned by report@snyk.io to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Link Following in juce-framework/JUCE | CVE		MISC snyk.io/vuln/SNYK-UNMANAGED-JUCEFRAMEWORKJUCE

Link Following in juce-framework/JUCE | CVE-2021-23521 | Snyk	snyk.io text/html	MISC snyk.io/vuln/SNYK-UNMANAGED-JUCEFRAMEWORKJUCE-2388608
ZipFile: Add path checks to uncompressEntry() · juce-framework/JUCE@2e874e8 · GitHub	github.com text/html	MISC github.com/juce-framework/JUCE/commit/2e874e80cba0152201aff6a4d0dc407997d10a7f

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

182357 Debian Security Update for juce (CVE-2021-23521)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:juce:juce:*:*:*:*:*:*:*:*:

Discovery Credit

Snyk Security Research Team

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-23521 : This affects the package juce-framework/JUCE before 6.1.5. This vulnerability is triggered when a… twitter.com/i/web/status/1…	2022-01-31 10:57:18
@SecRiskRptSME	RT: CVE-2021-23521 This affects the package juce-framework/JUCE before 6.1.5. This vulnerability is triggered when… twitter.com/i/web/status/1…	2022-01-31 12:33:32
/r/netcve	CVE-2021-23521	2022-01-31 12:38:40

← Previous ID

Next ID→