Snyk Vulnerability Database › Unmanaged (C/C++) › juce-framework/JUCE

Link Following

Affecting juce-framework/JUCE package, versions [,6.1.5)

Share ⌄

How to fix?

Upgrade `juce-framework/JUCE` to version 6.1.5 or higher.

Overview

`juce-framework/JUCE` is an open-source cross-platform C++ application framework for creating high quality desktop and mobile applications, including VST, VST3, AU, AUv3, RTAS and AAX audio plug-ins.
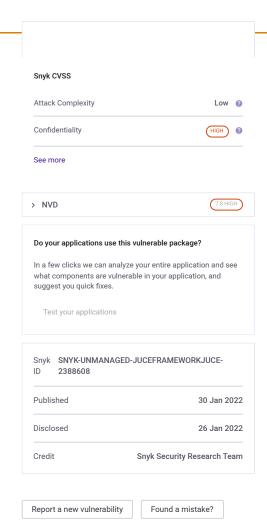
Affected versions of this package are vulnerable to Link Following. This vulnerability is triggered when a malicious archive is crafted with an entry containing a symbolic link. When extracted, the symbolic link is followed outside of the target dir allowing writing arbitrary files on the target host. 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.

References

- Github Commit

Snyk CVSS

Attack Complexity	Low ?
Confidentiality	HIGH ?

See more

> NVD   7.8 HIGH

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Report a new vulnerability   Found a mistake?

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information