MEDIUM

Search by package name or CVE

Arbitrary File Write via Archive Extraction (Zip Slip)

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

INTRODUCED: 26 JAN 2022 CVE-2021-23520 ? CWE-29 ? 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 Arbitrary File Write via Archive Extraction (Zip Slip) via the `ZipFile::uncompressEntry function` in `juce_ZipFile.cpp` . This vulnerability is triggered when the archive is extracted upon calling `uncompressTo()` on a ZipFile object.

Details

It is exploited using a specially crafted zip archive, that holds path traversal filenames. When exploited, a filename in a malicious archive is concatenated to the target extraction directory, which results in the final path ending up outside of the target folder. For instance, a zip may hold a file with a "../../file.exe" location and thus break out of the target folder. If an executable or a configuration file is overwritten with a file containing malicious code, the problem can turn into an arbitrary code execution issue quite easily.

The following is an example of a zip archive with one benign file and one malicious file. Extracting the malicous file will result in traversing out of the target folder, ending up in `/root/.ssh/` overwriting the `authorized_keys` file:

```
+2018-04-15 22:04:29 ..... 19 19 good.txt


+2018-04-15 22:04:42 ..... 20 20 ../../../../../../root/.ssh/authorized_keys
```

References

- Github Commit
- Zip Slip Advisory

Snyk CVSS

Attack Complexity	Low ?
User Interaction	Required ?
Integrity	HIGH ?

See more

NVD 9.8 CRITICAL

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

Snyk ID	SNYK-UNMANAGED-JUCEFRAMEWORKJUCE-2388607
Published	30 Jan 2022
Disclosed	26 Jan 2022
Credit	Snyk Security Research Team

Report a new vulnerability Found a mistake?

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon Join the >> community

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.