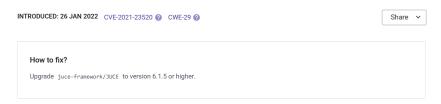
# **snyk** Vulnerability DB

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

## Arbitrary File Write via Archive Extraction (Zip Slip)

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



#### 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 <code>ZipFile::uncompressEntry</code> function in <code>juce\_ZipFile.cpp</code>. This vulnerability is triggered when the archive is extracted upon calling <code>uncompressTo()</code> 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.

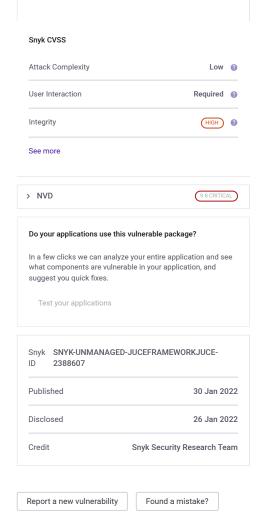
The following is an example of a zip archive with one benign file and one malicious file. Extracting the malicous file will result in traversing out of the target folder, ending up in /root/.ssh/ overwriting the authorized\_keys file:

```
+2818-04-15 22:04:29 ..... 19 19 good.txt

+2818-04-15 22:04:42 ..... 20 20 ../../../../root/.ssh/authorized.keys
```

### References

- Github Commit
- Zip Slip Advisory



Q Search by package name or CVE

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

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT





© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

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