snyk Vulnerability DB

CRITICAL

Snyk Vulnerability Database › npm › zip-local

Search by package name or CVE

Arbitrary File Write via Archive Extraction (Zip Slip)

Affecting zip-local package, versions <0.3.5

INTRODUCED: 29 DEC 2021 CVE-2021-23484 CWE-29 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `zip-local` to version 0.3.5 or higher.

Overview

zip-local is a to zip and unzip local directories

Affected versions of this package are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip) which can lead to an extraction of a crafted file outside the intended extraction directory.

PoC:

```
var zipper = require('zip-local'); zipper.unzip("zipslip.zip", function(error, unzipped) { if(!error) { //
extract to the current working directory unzipped.save(null, function() { }); var unzippedfs =
unzipped.memory(); } }); Execute the following commands 1. npm install zip-local # Install affected module
2. zipslip example file can be found at - https://github.com/snyk/zip-slip-
vulnerability/blob/master/archives/zip-slip.zip 3. node poc.js # Run the PoC
```

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
- Vulnerable Code

Snyk CVSS

Attack Complexity	Low
Confidentiality	HIGH
Integrity	HIGH
Availability	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-JS-ZIPLOCAL-2327477
Published	25 Jan 2022
Disclosed	29 Dec 2021
Credit	7he6uzzer

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

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

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