# Buffer Overflow vulnerability in Zlib::GzipReader

Low **hsbt** published **GHSA-g857-hhfv-j68w** 2 weeks ago

**Package**

**zlib** (RubyGems)

**Affected versions**

<= 3.2.2

**Patched versions**

3.0.1, 3.1.2, 3.2.3

**Description**

## Details

A buffer overflow vulnerability exists in `Zlib::GzipReader`.

The `zstream_buffer_ungets` function prepends caller-provided bytes ahead of previously produced output but fails to guarantee the backing Ruby string has enough capacity before the memmove shifts the existing data. This can lead to memory corruption when the buffer length exceeds capacity.

## Recommended action

We recommend to update the `zlib` gem to version 3.2.3 or later. In order to ensure compatibility with bundled version in older Ruby series, you may update as follows instead:

- For Ruby 3.2 users: Update to zlib 3.0.1
- For Ruby 3.3 users: Update to zlib 3.1.2

You can use gem update zlib to update it. If you are using bundler, please add `gem "zlib", ">= 3.2.3"` to your Gemfile.

## Affected versions

zlib gem 3.2.2 or lower

## Credits

calysteon

## References

- https://hackerone.com/reports/3467067

**Severity**

Low

**CVE ID**

CVE-2026-27820

**Weaknesses**

No CWEs