

pyca / cryptography Public[Code](#) [Issues 34](#) [Pull requests 20](#) [Actions](#) [Security and quality 15](#)

# Buffer overflow if non-contiguous buffers were passed to APIs

Moderate alex published GHSA-p423-j2cm-9vmq 19 hours ago

## Package

 cryptography (pip)

### Affected versions

&gt;=45.0.0

### Patched versions

&gt;=46.0.7

## Description

If a non-contiguous buffer was passed to APIs which accepted Python buffers (e.g. `Hash.update()`), this could lead to buffer overflows. For example:

```
h = Hash(SHA256())
b.update(buf[:-1])
```



would read past the end of the buffer on Python >3.11

## Severity

Moderate

## CVE ID

CVE-2026-39892

## Weaknesses

No CWEs