

[CVE-2025-4516] Use-after-free crash using bytes.decode("unicode_escape", error="ignore|replace")



[Seth Larson](#)

May 15, 2025 1:33 p.m.

There is a MEDIUM severity security issue in CPython when using `bytes.decode("unicode_escape", error="ignore|replace")`. The use-after-free being exploited would likely result in a crash.

If you are not using the "unicode_escape" encoding or an error handler your usage is not affected. To work-around this issue you may stop using the error= handler and instead wrap the bytes.decode() call in a try-except catching the decoding error.

Please see the linked CVE ID for the latest information on affected versions:

- <https://www.cve.org/CVERecord?id=CVE-2025-4516>
- <https://github.com/python/cpython/pull/129648>

Attachments:

[attachment.html](#) (text/html — 861 bytes)

[Reply](#)

0 0 A

[Show replies by date](#)



353

Age (days ago)

[List overview](#)

[Download](#)

0 comments

1 participants

[Add to favorites](#)

TAGS

353

Last active (days ago)

PARTICIPANTS (1)



Seth Larson



Powered by [HyperKitty](#) version 1.3.12.