

python / cpython Public

[Code](#) [Issues](#) 5k+ [Pull requests](#) 2.1k [Actions](#) [Projects](#) [Security and q](#)

New issue



Use-after-free in `unicode_escape` decoder with error handler #133767

Closed

Assignees



Labels

3.10

3.11

3.12

3.13

3.14

3.15

3.9 (EOL)

interpreter-core

release-blocker

topic-unicode

type-crash

type-security



sethmlarson opened on May 9, 2025 · edited by bedevere-app

Edits ▾

Contributor



Crash report

What happened?

When using `.decode("unicode_escape")` with an error handler there is a use-after-free segfault.

CPython versions tested on:

CPython main branch

Operating systems tested on:

No response

Output from running 'python -VV' on the command line:

No response

Linked PRs

- [gh-133767: Fix use-after-free in the unicode-escape decoder with an error handler #129648](#)

- [\[3.14\] gh-133767: Fix use-after-free in the unicode-escape decoder with an error handler \(GH-129648\) #133942](#)
- [\[3.13\] gh-133767: Fix use-after-free in the unicode-escape decoder with an error handler \(GH-129648\) #133944](#)
- [\[3.12\] Fix use-after-free in the unicode-escape decoder with error handler \(GH-133767\) #134255](#)
- [\[3.12\] gh-133767: Fix use-after-free in the unicode-escape decoder with an error handler \(GH-129648\) \(GH-133944\) #134337](#)
- [\[3.11\] gh-133767: Fix use-after-free in the unicode-escape decoder with an error handler \(GH-129648\) \(GH-133944\) #134341](#)
- [\[3.10\] gh-133767: Fix use-after-free in the unicode-escape decoder with an error handler \(GH-129648\) \(GH-133944\) #134345](#)
- [\[3.9\] gh-133767: Fix use-after-free in the unicode-escape decoder with an error handler \(GH-129648\) \(GH-133944\) #134346](#)

sethmlarson added **type-crash** on May 9, 2025

sethmlarson changed the title ~~Use-after-free in unicode-escape decoder with error handler~~ Use-after-free in `unicode_escape` decoder with error handler on May 9, 2025

serhiy-storchaka self-assigned this on May 9, 2025

bedevere-app mentioned this on May 9, 2025

[gh-133767: Fix use-after-free in the unicode-escape decoder with an error handler #129648](#)

picnixz added **interpreter-core** **topic-unicode** **type-security** **3.11** **3.10** **3.9 (EOL)** **3.12** **3.13** **3.14** **3.15** on May 10, 2025

serhiy-storchaka added a commit that references this issue on May 12, 2025

[gh-133767](#): Fix use-after-free in the unicode-escape decoder with an e.

Verified 9f69a58

38 remaining items

Load more

[Sign up for free](#) to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

Metadata



Assignees


 serhiy-storchaka

Labels

- 3.10
- 3.11
- 3.12
- 3.13
- 3.14
- 3.15
- 3.9 (EOL)
- interpreter-core
- release-blocker
- topic-unicode
- type-crash
- type-security

Projects

 **Release and Deferred blockers** 

Status Done 

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants

 +1

