[CVE-2025-8291] ZIP64 End of Central Directory (EOCD) Locator record offset not checked

Seth Larson

Oct. 7, 2025 6:06 p.m.

There is a MEDIUM severity vulnerability affecting CPython.

The 'zipfile' module would not check the validity of the ZIP64 End of Central Directory (EOCD) Locator record offset value would not be used to locate the ZIP64 EOCD record, instead the ZIP64 EOCD record would be assumed to be the previous record in the ZIP archive. This could be abused to create ZIP archives that are handled differently by the 'zipfile' module compared to other ZIP implementations.

Remediation maintains this behavior, but checks that the offset specified in the ZIP64 EOCD Locator record matches the expected value.

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

- https://www.cve.org/CVERecord?id=CVE-2025-8291
- https://github.com/python/cpython/pull/139702

Attachments:
attachment.html (text/html — 970 bytes)

0 0

Reply

Show replies by date

211
Age (days ago)

211
Last active (days ago)

List overview

Download

0 comments
1 participants

Add to favorites

TAGS

PARTICIPANTS (1)

Seth Larson