FITS GZIP decompression bomb in Pillow < 12.2.0

High **aclark4life** published **GHSA-whj4-6x5x-4v2j** 5 days ago

Package

pillow (pip)

Affected versions

>= 10.3.0, < 12.2.0

Patched versions

12.2.0

Description

Impact

Pillow did not limit the amount of GZIP-compressed data read when decoding a FITS image, making it vulnerable to decompression bomb attacks. A specially crafted FITS file could cause unbounded memory consumption, leading to denial of service (OOM crash or severe performance degradation).

Patches

The amount of data read is now limited to the necessary amount.
Fixed in Pillow 12.2.0 (PR #9521).

Workarounds

Avoid Pillow >= 10.3.0, < 12.2.0
Only open specific image formats, excluding FITS.

References

- #9521
- https://pillow.readthedocs.io/en/stable/releasenotes/12.2.0.html#prevent-fits-decompression-bomb

Severity

High

CVE ID

CVE-2026-40192

Weaknesses

▶ CWE-400

Credits

sammiee5311 Reporter