
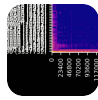


[Skip to main content](#) 1

[Skip to main navigation](#) 2

← Post 



sigd...
@si...

Security Advisory: CVE-2025-70103 - Heap-Based Buffer Overflow in libjxl / cjxl

A heap-based buffer overflow vulnerability was identified in JPEG XL libjxl when processing crafted PBM/PNM images.

Summary:
The vulnerability exists in ``jxl::extras::DecodelmagePNM()` in

Create account

Login



c`. When processing a specially crafted PBM/PNM image, insufficient validation of buffer sizes before memory copy operations may cause `memcpy()` to write past the end of an allocated heap buffer.

The issue was observed as a WRITE of 24 bytes at the end of a 16-byte heap region.

CWE:
CWE-122 -
Heap-based
Buffer
Overflow

[Create account](#)[Login](#)

bounds
Write

Affected
product:
JPEG XL /
libjxl

Affected
component

:
`lib/extras/
dec/pnm.c`
c`

Function:
`jxl::extras::
Decodelma
gePNM()`

Affected
line:
`pnm.cc:55`
4`

Affected
version:
The issue
was
reproduced
in `cjxl`
v0.12.0` at
commit
`24357f189`
c233c03fb`
46368a142`
a0b2c1a94`
9f9d`.

Attack
conditions:

Create account

Login

the vulnerable application or library consumer to process a crafted PBM/PNM image. This can be triggered locally via ``cjxl`` or through software that exposes the ``DecodemagePNM`` decoding path to attacker-controlled input.

Example reproduction command:
``. /cjxl ./2_PBM_lib_extras_dec_pnm_cc_554 --disable_output``

Impact:

[Create account](#)[Login](#)

n may cause memory corruption and process termination . The confirmed impact is denial of service (DoS) due to a crash during image processing . No evidence of reliable arbitrary code execution has been identified.

Fix / mitigation status:
The upstream issue is closed. A mitigation/fix proposal was provided in PR

[Create account](#)[Login](#)

additional
buffer-size,
row-
boundary,
pixel-size,
offset, and
extra-
channel
checks.
Users are
advised to
update to a
libjxl build
that
contains
the
relevant fix
once
available,
or review
and apply
the
mitigation
from PR
`#4338`
where
appropriate
.

References

:

Issue:

[github.com
/libjxl/libjxl
/issue...](https://github.com/libjxl/libjxl/issue...)

Fix /
mitigation
PR:

Create account

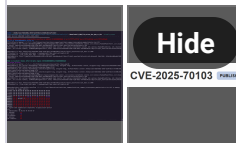
Login

[/pull/...](#)
[github.com](#)
[/libjxl/libjxl](#)
[/commi...](#)

PoC:
[github.com](#)
[/sigdevel/p](#)
[ocs/blob/...](#)

Credit:
[@sigdevel](#)

[cve.org/CV](#)
[ERecord?](#)
[id=CVE-](#)
[2025-...](#)



[#fuzzing](#)

[#infosec](#)

[#security](#)

...and 9 more

May
26,
2026, · · We
06:14
PM

Last edited
May 27, 07:22
PM

0 boosts · 0 qu



Create account

Login