Integer overflow in DWA setupChannelData planarUncRle pointer arithmetic (missed variant of CVE-2026-34589)

High **cary-ilm** published **GHSA-j526-66f6-fxhx** 2 days ago

Package

OpenEXR

Affected versions

3.2.0–3.2.7, 3.3.0–3.3.9, 3.4.0–3.4.9

Patched versions

3.2.8, 3.3.10, 3.4.10

Description

Summary

`internal_dwa_compressor.h:1722` performs `curc->width * curc->height` in `int32` arithmetic without a `(size_t)` cast. This is the same overflow pattern fixed in other locations by the recent CVE-2026-34589 batch, but this line was missed.

Details

In DWA `setupChannelData`, line 1722:

```
cd->planarUncRle[byte] =
    cd->planarUncRle[byte - 1] + curc->width * curc->height;
```

Both `curc->width` and `curc->height` are `int32_t`. For dimensions where `width * height > INT32_MAX`, the multiplication wraps. The result is used as a byte offset from the previous plane's buffer pointer, causing `planarUncRle[byte]` to point inside or before the allocated buffer instead of after it.

When RLE decoding later writes through these pointers, it corrupts heap memory.

Compare with line 1699 in the same function, which was already fixed:

```
uncSize = (size_t) curc->width * (size_t) curc->height * ...
```

Line 1699 has casts. Line 1722 does not.

Reachability

```
Crafted EXR (DWAA/DWAB compression, width*height > INT32_MAX)
  → exr_decoding_run()
  → internal_exr_undo_dwa() → DwaCompressor_uncompress()
  → setupChannelData for non-DCT (RLE) channels
  → line 1722: int32 overflow in planarUncRle pointer offset
  → aliased plane pointers → heap corruption during RLE decode
```

Triggered for channels not in a CSC set (non-DCT path), which includes any UINT or single-channel layout.

Suggested fix

```
cd->planarUncRle[byte] =
    cd->planarUncRle[byte - 1] + (size_t) curc->width * (size_t) curc->height;
```

Impact

Heap buffer corruption when opening a crafted DWAA/DWAB EXR file with large dimensions on non-DCT channels. Same impact class as CVE-2026-34589.

Severity

High 8.4 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Local
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User interaction	Active

Vulnerable System Impact Metrics	
Confidentiality	High
Integrity	High
Availability	High
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVE ID

CVE-2026-40244

Weaknesses

▶ CWE-190

Credits

Medoedus Reporter