59260 | diff (/project/ffmpeg/patch/177766314111.63.10674887811034989327@29965ddac10e/raw/)

mbox (/project/ffmpeg/patch/177766314111.63.10674887811034989327@29965ddac10e/mbox/)

series (/series/17747/mbox/)

[FFmpeg-devel,PR] avcodec/rasc: fix heap use-after-free in decode_move() (PR #22992)

Message ID	177766314111.63.10674887811034989327@29965ddac10e
State	New
Headers	show
Series	[FFmpeg-devel,PR] avcodec/rasc: fix heap use-after-free in decode_move() (PR #22992) (/project/ffmpeg/list/?series=17747) | expand

Commit Message

qwerzoid (/project/ffmpeg/list/?submitter=1995) May 1, 2026, 7:19 p.m. UTC

```
PR #22992 opened by michaelni
URL: https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/22992
Patch URL: https://code.ffmpeg.org/FFmpeg/FFmpeg/pulls/22992.patch

Use a separate scratch buffer (s->mv_scratch) for the type-0 pixel
copy so s->delta and mc are not disturbed for the lifetime of
decode_move().  The new buffer is freed in decode_close().

Found-by: Seung Min Shin
Patch based on suggsted fix by Seung Min Shin

Signed-off-by: Michael Niedermayer <michael@niedermayer.cc>


>From 56ee3ee03055cb514457eb45833671f8ab9ff75b Mon Sep 17 00:00:00 2001
From: Michael Niedermayer <michael@niedermayer.cc>
Date: Fri, 1 May 2026 20:31:57 +0200
Subject: [PATCH] avcodec/rasc: fix heap use-after-free in decode_move()

Use a separate scratch buffer (s->mv_scratch) for the type-0 pixel
copy so s->delta and mc are not disturbed for the lifetime of
decode_move().  The new buffer is freed in decode_close().

Found-by: Seung Min Shin
Patch based on suggsted fix by Seung Min Shin

Signed-off-by: Michael Niedermayer <michael@niedermayer.cc>
---
 libavcodec/rasc.c | 10 ++++++----
 1 file changed, 6 insertions(+), 4 deletions(-)
```

59260 | diff (/project/ffmpeg/patch/177766314111.63.10674887811034989327@29965ddac10e/raw/)

mbox (/project/ffmpeg/patch/177766314111.63.10674887811034989327@29965ddac10e/mbox/)

series (/series/17747/mbox/)

Patch

```
diff --git a/libavcodec/rasc.c b/libavcodec/rasc.c
index a8e00a41a6..5f956a9b2c 100644
--- a/libavcodec/rasc.c
+++ b/libavcodec/rasc.c
@@ -51,6 +51,8 @@  typedef struct RASCContext {
     GetByteContext  gb;
     uint8_t        *delta;
     int             delta_size;
+    uint8_t        *mv_scratch;
+    unsigned int    mv_scratch_size;
     uint8_t        *cursor;
     int             cursor_size;
     unsigned        cursor_w;
@@ -294,10 +296,8 @@  static int decode_move(AVCodecContext *avctx,
                 b2 -= s->frame2->linesize[0];
             }
         } else if (type == 0) {
-            uint8_t *buffer;
-
-            av_fast_padded_malloc(&s->delta, &s->delta_size, w * h * s->bpp);
-            buffer = s->delta;
+            av_fast_padded_malloc(&s->mv_scratch, &s->mv_scratch_size, w * h * s->bpp);
+            uint8_t *buffer = s->mv_scratch;
             if (!buffer)
                 return AVERROR(ENOMEM);

@@ -772,6 +772,8 @@  static av_cold int decode_close(AVCodecContext *avctx)
     s->cursor_size = 0;
     av_freep(&s->delta);
     s->delta_size = 0;
+    av_freep(&s->mv_scratch);
+    s->mv_scratch_size = 0;
     av_frame_free(&s->frame1);
     av_frame_free(&s->frame2);
     ff_inflate_end(&s->zstream);
```