#8295 closed defect (fixed)

Opened 3 years ago
Closed 3 years ago

memory leaks in url_open_dyn_buf_internal()

Reported by:	Suhwan	Owned by:	
Priority:	important	Component:	avformat
Version:	git-master	Keywords:	
Cc:		Blocked By:	
Blocking:		Reproduced by developer:	no
Analyzed by developer:	no		

Description

Summary of the bug:
There are memory leaks in url_open_dyn_buf_internal()
How to reproduce:

```
% ffmpeg_g -y -i $PoC tmp.nut

ffmpeg version N-95425-g1e35519fe0 Copyright (c) 2000-2019 the FFmpeg developers
built with clang version 6.0.0-1ubuntu2 (tags/RELEASE_600/final)
configuration: --cc=clang --cxx=clang++ --ld=clang --enable-debug
```

Here's Valgrind log

```
==38914== HEAP SUMMARY:
==38914==     in use at exit: 1,352 bytes in 3 blocks
==38914==   total heap usage: 4,302 allocs, 4,299 frees, 12,611,962 bytes allocate
==38914==
==38914== 1,320 (264 direct, 1,056 indirect) bytes in 1 blocks are definitely lost
==38914==    at 0x9FDFE76: memalign (in /usr/lib/valgrind/vgpreload_memcheck-amd64
==38914==    by 0x9FDFF91: posix_memalign (in /usr/lib/valgrind/vgpreload_memcheck
==38914==    by 0x592BD8D: av_malloc (mem.c:87)
==38914==    by 0x147F261: avio_alloc_context (aviobuf.c:140)
==38914==    by 0x147F261: url_open_dyn_buf_internal (aviobuf.c:1419)
==38914==    by 0x186E4AD: nut_write_trailer (nutenc.c:1173)
==38914==    by 0x17EBB33: av_write_trailer (mux.c:1283)
==38914==    by 0x48FF5B: transcode (ffmpeg.c:4716)
==38914==    by 0x487DA3: main (ffmpeg.c:4884)
==38914==
==38914== LEAK SUMMARY:
==38914==    definitely lost: 264 bytes in 1 blocks
==38914==    indirectly lost: 1,056 bytes in 1 blocks
==38914==      possibly lost: 0 bytes in 0 blocks
==38914==    still reachable: 32 bytes in 1 blocks
==38914==         suppressed: 0 bytes in 0 blocks
==38914== Reachable blocks (those to which a pointer was found) are not shown.
==38914== To see them, rerun with: --leak-check=full --show-leak-kinds=all
==38914==
==38914== For counts of detected and suppressed errors, rerun with: -v
==38914== ERROR SUMMARY: 82534 errors from 137 contexts (suppressed: 0 from 0)
```

ASAN log.

```
=================================================================
==21625==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 264 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x85c1021 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x1cdb48f in avio_alloc_context ffmpeg/libavformat/aviobuf.c:140:22
    #3 0x1cdb48f in url_open_dyn_buf_internal ffmpeg/libavformat/aviobuf.c:1419

Indirect leak of 1056 byte(s) in 1 object(s) allocated from:
    #0 0x4de9e8 in posix_memalign (ffmpeg_usan+0x4de9e8)
    #1 0x85c2178 in av_malloc ffmpeg/libavutil/mem.c:87:9
    #2 0x85c2178 in av_mallocz ffmpeg/libavutil/mem.c:238
    #3 0x1cdb3af in url_open_dyn_buf_internal ffmpeg/libavformat/aviobuf.c:1415:9
    #4 0x8a78fcd in _fini (ffmpeg_usan+0x8a78fcd)

SUMMARY: AddressSanitizer: 1320 byte(s) leaked in 2 allocation(s).
```

Please confirm.
Thanks

Attachments (1)

- PoC_url(14.4 KB) - added by Suhwan 3 years ago.

Change History (2)

by Suhwan, 3 years ago

Attachment: *PoC_url*added

comment:1 by James, 3 years ago

Component: undetermined → avformat
Resolution: → fixed
Status: new → closed

Fixed in 1d479300cbe0522c233b7d51148aea2b29bd29ad.

Note: See TracTickets for help on using tickets.