Exiv2 - Bug #1052

WAV file problem

08 Apr 2015 12:03 - Martin Pučálka

Status:	New	**Start date:**	08 Apr 2015
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	video	**Estimated time:**	0.00 hour
Target version:	0.28		

Description

Try to read exif data of some VAW files causes fall of my application.
Few days ago I got segmentation fault when i tried to read webm files. (Soluted here: [[http://dev.exiv2.org/issues/1033]])
I checked actual version from repository, build it and webm files are now Ok, but my VAW files still causes error.
Below is error I get, trying to print metadata using code in example ([[http://www.exiv2.org/doc/exifprint_8cpp-example.html]])
Please correct me, if I'm doing something wrong.

I will attach one of problematic VAW file.

- Error in `./a': free(): invalid next size (normal): 0x00000000008d4780 *** ======= Backtrace: =========
  /lib64/libc.so.6(+0x7850e)[0x7f6dcf71750e]
  /lib64/libc.so.6(cfree+0x5b5)[0x7f6dcf723165]
  /lib/libexiv2.so.13(*ZN5Exiv29RiffVideo15infoTagsHandlerEv+0x256)[0x7f6dd03fa006]*
  /lib/libexiv2.so.13(_ZN5Exiv29RiffVideo11decodeBlockEv+0x105)[0x7f6dd03fde35]
  /lib/libexiv2.so.13(_ZN5Exiv29RiffVideo10tagDecoderERNS_7DataBufEm+0x58)[0x7f6dd03fda88]
  /lib/libexiv2.so.13(_ZN5Exiv29RiffVideo11decodeBlockEv+0x105)[0x7f6dd03fde35]
  /lib/libexiv2.so.13(_ZN5Exiv29RiffVideo12readMetadataEv+0x348)[0x7f6dd03fe1c8]
  ./a[0x401719]
  /lib64/libc.so.6(_libc_start_main+0xf0)[0x7f6dcf6befe0]
  ./a[0x401509] ======= Memory map: ========
  00400000-00404000 r-xp 00000000 fd:02 1183361 /home/martin/ode/a
  00603000-00604000 r--p 00003000 fd:02 1183361 /home/martin/ode/a
  00604000-00605000 rw-p 00004000 fd:02 1183361 /home/martin/ode/a
  008d2000-008f3000 rw-p 00000000 00:00 0 [heap]
  7f6dcab41000-7f6dcabb9000 r-xp 00000000 fd:00 132107 /usr/lib64/libfreebl3.so
  7f6dcabb9000-7f6dcadb8000 ---p 00078000 fd:00 132107 /usr/lib64/libfreebl3.so
  7f6dcadb8000-7f6dcadba000 r--p 00077000 fd:00 132107 /usr/lib64/libfreebl3.so
  7f6dcadba000-7f6dcadbb000 rw-p 00079000 fd:00 132107 /usr/lib64/libfreebl3.so
  7f6dcadbb000-7f6dcadbf000 rw-p 00000000 00:00 0
  7f6dcadbf000-7f6dcade3000 r-xp 00000000 fd:00 140602 /usr/lib64/liblzma.so.5.0.99
  7f6dcade3000-7f6dcafe2000 ---p 00024000 fd:00 140602 /usr/lib64/liblzma.so.5.0.99
  7f6dcafe2000-7f6dcafe3000 r--p 00023000 fd:00 140602 /usr/lib64/liblzma.so.5.0.99
  7f6dcafe3000-7f6dcafe4000 rw-p 00024000 fd:00 140602 /usr/lib64/liblzma.so.5.0.99
  7f6dcafe4000-7f6dcb050000 r-xp 00000000 fd:00 139407 /usr/lib64/libpcre.so.1.2.3
  7f6dcb050000-7f6dcb24f000 ---p 0006c000 fd:00 139407 /usr/lib64/libpcre.so.1.2.3
  7f6dcb24f000-7f6dcb250000 r--p 0006b000 fd:00 139407 /usr/lib64/libpcre.so.1.2.3
  7f6dcb250000-7f6dcb251000 rw-p 0006c000 fd:00 139407 /usr/lib64/libpcre.so.1.2.3
  7f6dcb251000-7f6dcb258000 r-xp 00000000 fd:00 138916 /usr/lib64/libcrypt-2.20.so
  7f6dcb258000-7f6dcb457000 ---p 00007000 fd:00 138916 /usr/lib64/libcrypt-2.20.so
  7f6dcb457000-7f6dcb458000 r--p 00006000 fd:00 138916 /usr/lib64/libcrypt-2.20.so
  7f6dcb458000-7f6dcb459000 rw-p 00007000 fd:00 138916 /usr/lib64/libcrypt-2.20.so
  7f6dcb459000-7f6dcb487000 rw-p 00000000 00:00 0
  7f6dcb487000-7f6dcb4a9000 r-xp 00000000 fd:00 140845 /usr/lib64/libselinux.so.1
  7f6dcb4a9000-7f6dcb6a8000 ---p 00022000 fd:00 140845 /usr/lib64/libselinux.so.1
  7f6dcb6a8000-7f6dcb6a9000 r--p 00021000 fd:00 140845 /usr/lib64/libselinux.so.1
  7f6dcb6a9000-7f6dcb6aa000 rw-p 00022000 fd:00 140845 /usr/lib64/libselinux.so.1
  7f6dcb6aa000-7f6dcb6ac000 rw-p 00000000 00:00 0
  7f6dcb6ac000-7f6dcb6c8000 r-xp 00000000 fd:00 140837 /usr/lib64/libsasl2.so.3.0.0
  7f6dcb6c8000-7f6dcb8c7000 ---p 0001c000 fd:00 140837 /usr/lib64/libsasl2.so.3.0.0
  7f6dcb8c7000-7f6dcb8c8000 r--p 0001b000 fd:00 140837 /usr/lib64/libsasl2.so.3.0.0
  7f6dcb8c8000-7f6dcb8c9000 rw-p 0001c000 fd:00 140837 /usr/lib64/libsasl2.so.3.0.0
  7f6dcb8c9000-7f6dcb8e0000 r-xp 00000000 fd:00 139440 /usr/lib64/libresolv-2.20.so
  7f6dcb8e0000-7f6dcbadf000 ---p 00017000 fd:00 139440 /usr/lib64/libresolv-2.20.so

7f6dcbadf000-7f6dcbae0000 r--p 00016000 fd:00 139440 /usr/lib64/libresolv-2.20.so
7f6dcbae0000-7f6dcbae1000 rw-p 00017000 fd:00 139440 /usr/lib64/libresolv-2.20.so
7f6dcbae1000-7f6dcbae3000 rw-p 00000000 00:00 0
7f6dcbae3000-7f6dcbae6000 r-xp 00000000 fd:00 140579 /usr/lib64/libkeyutils.so.1.5
7f6dcbae6000-7f6dcbce5000 ---p 00003000 fd:00 140579 /usr/lib64/libkeyutils.so.1.5
7f6dcbce5000-7f6dcbce6000 r--p 00002000 fd:00 140579 /usr/lib64/libkeyutils.so.1.5
7f6dcbce6000-7f6dcbce7000 rw-p 00003000 fd:00 140579 /usr/lib64/libkeyutils.so.1.5
7f6dcbce7000-7f6dcbcf5000 r-xp 00000000 fd:00 140585 /usr/lib64/libkrb5support.so.0.1
7f6dcbcf5000-7f6dcbef4000 ---p 0000e000 fd:00 140585 /usr/lib64/libkrb5support.so.0.1
7f6dcbef4000-7f6dcbef5000 r--p 0000d000 fd:00 140585 /usr/lib64/libkrb5support.so.0.1
7f6dcbef5000-7f6dcbef6000 rw-p 0000e000 fd:00 140585 /usr/lib64/libkrb5support.so.0.1
7f6dcbef6000-7f6dcbf45000 r-xp 00000000 fd:00 140590 /usr/lib64/libldap-2.4.so.2.10.3
7f6dcbf45000-7f6dcc144000 ---p 0004f000 fd:00 140590 /usr/lib64/libldap-2.4.so.2.10.3
7f6dcc144000-7f6dcc147000 r--p 0004e000 fd:00 140590 /usr/lib64/libldap-2.4.so.2.10.3
7f6dcc147000-7f6dcc148000 rw-p 00051000 fd:00 140590 /usr/lib64/libldap-2.4.so.2.10.3
7f6dcc148000-7f6dcc156000 r-xp 00000000 fd:00 140588 /usr/lib64/liblber-2.4.so.2.10.3
7f6dcc156000-7f6dcc355000 ---p 0000e000 fd:00 140588 /usr/lib64/liblber-2.4.so.2.10.3
7f6dcc355000-7f6dcc356000 r--p 0000d000 fd:00 140588 /usr/lib64/liblber-2.4.so.2.10.3
7f6dcc356000-7f6dcc357000 rw-p 0000e000 fd:00 140588 /usr/lib64/liblber-2.4.so.2.10.3
7f6dcc357000-7f6dcc36e000 r-xp 00000000 fd:00 139365 /usr/lib64/libpthread-2.20.so
7f6dcc36e000-7f6dcc56d000 ---p 00017000 fd:00 139365 /usr/lib64/libpthread-2.20.so
7f6dcc56d000-7f6dcc56e000 r--p 00016000 fd:00 139365 /usr/lib64/libpthread-2.20.so
7f6dcc56e000-7f6dcc56f000 rw-p 00017000 fd:00 139365 /usr/lib64/libpthread-2.20.so
7f6dcc56f000-7f6dcc573000 rw-p 00000000 00:00 0
7f6dcc573000-7f6dcc5ad000 r-xp 00000000 fd:00 140672 /usr/lib64/libnspr4.so
7f6dcc5ad000-7f6dcc7ad000 ---p 0003a000 fd:00 140672 /usr/lib64/libnspr4.so
7f6dcc7ad000-7f6dcc7ae000 r--p 0003a000 fd:00 140672 /usr/lib64/libnspr4.so
7f6dcc7ae000-7f6dcc7b0000 rw-p 0003b000 fd:00 140672 /usr/lib64/libnspr4.so
7f6dcc7b0000-7f6dcc7b2000 rw-p 00000000 00:00 0
7f6dcc7b2000-7f6dcc7b6000 r-xp 00000000 fd:00 140753 /usr/lib64/libplc4.so
7f6dcc7b6000-7f6dcc9b5000 ---p 00004000 fd:00 140753 /usr/lib64/libplc4.so
7f6dcc9b5000-7f6dcc9b6000 r--p 00003000 fd:00 140753 /usr/lib64/libplc4.so
7f6dcc9b6000-7f6dcc9b7000 rw-p 00004000 fd:00 140753 /usr/lib64/libplc4.so
7f6dcc9b7000-7f6dcc9ba000 r-xp 00000000 fd:00 140754 /usr/lib64/libplds4.so
7f6dcc9ba000-7f6dccbb9000 ---p 00003000 fd:00 140754 /usr/lib64/libplds4.so
7f6dccbb9000-7f6dccbba000 r--p 00002000 fd:00 140754 /usr/lib64/libplds4.so
7f6dccbba000-7f6dccbbb000 rw-p 00003000 fd:00 140754 /usr/lib64/libplds4.so
7f6dccbbb000-7f6dccbe1000 r-xp 00000000 fd:00 140695 /usr/lib64/libnssutil3.so
7f6dccbe1000-7f6dccde0000 ---p 00026000 fd:00 140695 /usr/lib64/libnssutil3.so
7f6dccde0000-7f6dccde6000 r--p 00025000 fd:00 140695 /usr/lib64/libnssutil3.so
7f6dccde6000-7f6dccde7000 rw-p 0002b000 fd:00 140695 /usr/lib64/libnssutil3.so
7f6dccde7000-7f6dccf05000 r-xp 00000000 fd:00 140673 /usr/lib64/libnss3.so
7f6dccf05000-7f6dcd105000 ---p 0011e000 fd:00 140673 /usr/lib64/libnss3.so
7f6dcd105000-7f6dcd10a000 r--p 0011e000 fd:00 140673 /usr/lib64/libnss3.so
7f6dcd10a000-7f6dcd10c000 rw-p 00123000 fd:00 140673 /usr/lib64/libnss3.so
7f6dcd10c000-7f6dcd10e000 rw-p 00000000 00:00 0
7f6dcd10e000-7f6dcd132000 r-xp 00000000 fd:00 140861 /usr/lib64/libsmime3.so
7f6dcd132000-7f6dcd331000 ---p 00024000 fd:00 140861 /usr/lib64/libsmime3.so
7f6dcd331000-7f6dcd334000 r--p 00023000 fd:00 140861 /usr/lib64/libsmime3.so
7f6dcd334000-7f6dcd335000 rw-p 00026000 fd:00 140861 /usr/lib64/libsmime3.so
7f6dcd335000-7f6dcd370000 r-xp 00000000 fd:00 140884 /usr/lib64/libssl3.so
7f6dcd370000-7f6dcd56f000 ---p 0003b000 fd:00 140884 /usr/lib64/libssl3.so
7f6dcd56f000-7f6dcd572000 r--p 0003a000 fd:00 140884 /usr/lib64/libssl3.so
7f6dcd572000-7f6dcd573000 rw-p 0003d000 fd:00 140884 /usr/lib64/libssl3.so
7f6dcd573000-7f6dcd574000 rw-p 00000000 00:00 0
7f6dcd574000-7f6dcd59c000 r-xp 00000000 fd:00 140882 /usr/lib64/libssh2.so.1.0.1
7f6dcd59c000-7f6dcd79b000 ---p 00028000 fd:00 140882 /usr/lib64/libssh2.so.1.0.1
7f6dcd79b000-7f6dcd79c000 r--p 00027000 fd:00 140882 /usr/lib64/libssh2.so.1.0.1
7f6dcd79c000-7f6dcd79d000 rw-p 00028000 fd:00 140882 /usr/lib64/libssh2.so.1.0.1
7f6dcd79d000-7f6dcd7cf000 r-xp 00000000 fd:00 140541 /usr/lib64/libidn.so.11.6.11
7f6dcd7cf000-7f6dcd9cf000 ---p 00032000 fd:00 140541 /usr/lib64/libidn.so.11.6.11
7f6dcd9cf000-7f6dcd9d0000 r--p 00032000 fd:00 140541 /usr/lib64/libidn.so.11.6.11
7f6dcd9d0000-7f6dcd9d1000 rw-p 00033000 fd:00 140541 /usr/lib64/libidn.so.11.6.11
7f6dcd9d1000-7f6dcd9d4000 r-xp 00000000 fd:00 138935 /usr/lib64/libcom_err.so.2.1
7f6dcd9d4000-7f6dcdbd3000 ---p 00003000 fd:00 138935 /usr/lib64/libcom_err.so.2.1
7f6dcdbd3000-7f6dcdbd4000 r--p 00002000 fd:00 138935 /usr/lib64/libcom_err.so.2.1
7f6dcdbd4000-7f6dcdbd5000 rw-p 00003000 fd:00 138935 /usr/lib64/libcom_err.so.2.1

```
7f6dcdbd5000-7f6dcdc05000 r-xp 00000000 fd:00 140574                     /usr/lib64/libk5crypto.so.3.1
7f6dcdc05000-7f6dcde04000 ---p 00030000 fd:00 140574                     /usr/lib64/libk5crypto.so.3.1
7f6dcde04000-7f6dcde06000 r--p 0002f000 fd:00 140574                     /usr/lib64/libk5crypto.so.3.1
7f6dcde06000-7f6dcde07000 rw-p 00031000 fd:00 140574                     /usr/lib64/libk5crypto.so.3.1
7f6dcde07000-7f6dcde08000 rw-p 00000000 00:00 0
7f6dcde08000-7f6dcdedb000 r-xp 00000000 fd:00 140584                     /usr/lib64/libkrb5.so.3.3
7f6dcdedb000-7f6dce0da000 ---p 000d3000 fd:00 140584                     /usr/lib64/libkrb5.so.3.3
7f6dce0da000-7f6dce0e8000 r--p 000d2000 fd:00 140584                     /usr/lib64/libkrb5.so.3.3
7f6dce0e8000-7f6dce0eb000 rw-p 000e0000 fd:00 140584                     /usr/lib64/libkrb5.so.3.3
7f6dce0eb000-7f6dce134000 r-xp 00000000 fd:00 140436                     /usr/lib64/libgssapi_krb5.so.2.2
7f6dce134000-7f6dce334000 ---p 00049000 fd:00 140436                     /usr/lib64/libgssapi_krb5.so.2.2
7f6dce334000-7f6dce336000 r--p 00049000 fd:00 140436                     /usr/lib64/libgssapi_krb5.so.2.2
7f6dce336000-7f6dce338000 rw-p 0004b000 fd:00 140436                     /usr/lib64/libgssapi_krb5.so.2.2
7f6dce338000-7f6dce4f8000 r-xp 00000000 fd:00 138706                     /usr/lib64/libcrypto.so.1.0.1k
7f6dce4f8000-7f6dce6f7000 ---p 001c0000 fd:00 138706                     /usr/lib64/libcrypto.so.1.0.1k
7f6dce6f7000-7f6dce714000 r--p 001bf000 fd:00 138706                     /usr/lib64/libcrypto.so.1.0.1k
7f6dce714000-7f6dce721000 rw-p 001dc000 fd:00 138706                     /usr/lib64/libcrypto.so.1.0.1k
7f6dce721000-7f6dce725000 rw-p 00000000 00:00 0
7f6dce725000-7f6dce789000 r-xp 00000000 fd:00 138944                     /usr/lib64/libssl.so.1.0.1k
7f6dce789000-7f6dce989000 ---p 00064000 fd:00 138944                     /usr/lib64/libssl.so.1.0.1k
7f6dce989000-7f6dce98d000 r--p 00064000 fd:00 138944                     /usr/lib64/libssl.so.1.0.1k
7f6dce98d000-7f6dce994000 rw-p 00068000 fd:00 138944                     /usr/lib64/libssl.so.1.0.1k
7f6dce994000-7f6dce99b000 r-xp 00000000 fd:00 139476                     /usr/lib64/librt-2.20.so
7f6dce99b000-7f6dceb9a000 ---p 00007000 fd:00 139476                     /usr/lib64/librt-2.20.so
7f6dceb9a000-7f6dceb9b000 r--p 00006000 fd:00 139476                     /usr/lib64/librt-2.20.so
7f6dceb9b000-7f6dceb9c000 rw-p 00007000 fd:00 139476                     /usr/lib64/librt-2.20.so
7f6dceb9c000-7f6dceb9f000 r-xp 00000000 fd:00 138943                     /usr/lib64/libdl-2.20.so
7f6dceb9f000-7f6dced9e000 ---p 00003000 fd:00 138943                     /usr/lib64/libdl-2.20.so
7f6dced9e000-7f6dced9f000 r--p 00002000 fd:00 138943                     /usr/lib64/libdl-2.20.so
7f6dced9f000-7f6dceda0000 rw-p 00003000 fd:00 138943                     /usr/lib64/libdl-2.20.so
7f6dceda0000-7f6dcedc6000 r-xp 00000000 fd:00 140311                     /usr/lib64/libexpat.so.1.6.0
7f6dcedc6000-7f6dcefc6000 ---p 00026000 fd:00 140311                     /usr/lib64/libexpat.so.1.6.0
7f6dcefc6000-7f6dcefc9000 r--p 00026000 fd:00 140311                     /usr/lib64/libexpat.so.1.6.0
7f6dcefc9000-7f6dcefca000 rw-p 00029000 fd:00 140311                     /usr/lib64/libexpat.so.1.6.0
7f6dcefca000-7f6dcf039000 r-xp 00000000 fd:00 140244                     /usr/lib64/libcurl.so.4.3.0
7f6dcf039000-7f6dcf238000 ---p 0006f000 fd:00 140244                     /usr/lib64/libcurl.so.4.3.0
7f6dcf238000-7f6dcf23b000 r--p 0006e000 fd:00 140244                     /usr/lib64/libcurl.so.4.3.0
7f6dcf23b000-7f6dcf23c000 rw-p 00071000 fd:00 140244                     /usr/lib64/libcurl.so.4.3.0
7f6dcf23c000-7f6dcf23d000 rw-p 00000000 00:00 0
7f6dcf23d000-7f6dcf287000 r-xp 00000000 fd:00 155203                     /usr/lib64/libssh.so.4.4.1
7f6dcf287000-7f6dcf486000 ---p 0004a000 fd:00 155203                     /usr/lib64/libssh.so.4.4.1
7f6dcf486000-7f6dcf487000 r--p 00049000 fd:00 155203                     /usr/lib64/libssh.so.4.4.1
7f6dcf487000-7f6dcf489000 rw-p 0004a000 fd:00 155203                     /usr/lib64/libssh.so.4.4.1
7f6dcf489000-7f6dcf49e000 r-xp 00000000 fd:00 141101                     /usr/lib64/libz.so.1.2.8
7f6dcf49e000-7f6dcf69d000 ---p 00015000 fd:00 141101                     /usr/lib64/libz.so.1.2.8
7f6dcf69d000-7f6dcf69e000 r--p 00014000 fd:00 141101                     /usr/lib64/libz.so.1.2.8
7f6dcf69e000-7f6dcf69f000 rw-p 00015000 fd:00 141101                     /usr/lib64/libz.so.1.2.8
7f6dcf69f000-7f6dcf853000 r-xp 00000000 fd:00 138833                     /usr/lib64/libc-2.20.so
7f6dcf853000-7f6dcfa52000 ---p 001b4000 fd:00 138833                     /usr/lib64/libc-2.20.so
7f6dcfa52000-7f6dcfa56000 r--p 001b3000 fd:00 138833                     /usr/lib64/libc-2.20.so
7f6dcfa56000-7f6dcfa58000 rw-p 001b7000 fd:00 138833                     /usr/lib64/libc-2.20.so
7f6dcfa58000-7f6dcfa5c000 rw-p 00000000 00:00 0
7f6dcfa5c000-7f6dcfa72000 r-xp 00000000 fd:00 143063                     /usr/lib64/libgcc_s-4.9.2-20150212.so.1
7f6dcfa72000-7f6dcfc71000 ---p 00016000 fd:00 143063                     /usr/lib64/libgcc_s-4.9.2-20150212.so.1
7f6dcfc71000-7f6dcfc72000 r--p 00015000 fd:00 143063                     /usr/lib64/libgcc_s-4.9.2-20150212.so.1
7f6dcfc72000-7f6dcfc73000 rw-p 00016000 fd:00 143063                     /usr/lib64/libgcc_s-4.9.2-20150212.so.1
7f6dcfc73000-7f6dcfd7a000 r-xp 00000000 fd:00 138966                     /usr/lib64/libm-2.20.so
7f6dcfd7a000-7f6dcff79000 ---p 00107000 fd:00 138966                     /usr/lib64/libm-2.20.so
7f6dcff79000-7f6dcff7a000 r--p 00106000 fd:00 138966                     /usr/lib64/libm-2.20.so
7f6dcff7a000-7f6dcff7b000 rw-p 00107000 fd:00 138966                     /usr/lib64/libm-2.20.so
7f6dcff7b000-7f6dd006b000 r-xp 00000000 fd:00 139542                     /usr/lib64/libstdc++.so.6.0.20
7f6dd006b000-7f6dd026b000 ---p 000f0000 fd:00 139542                     /usr/lib64/libstdc++.so.6.0.20
7f6dd026b000-7f6dd0273000 r--p 000f0000 fd:00 139542                     /usr/lib64/libstdc++.so.6.0.20
7f6dd0273000-7f6dd0275000 rw-p 000f8000 fd:00 139542                     /usr/lib64/libstdc++.so.6.0.20
7f6dd0275000-7f6dd028a000 rw-p 00000000 00:00 0
7f6dd028a000-7f6dd053e000 r-xp 00000000 fd:00 527730                     /usr/local/lib/libexiv2.so.13.0.0
7f6dd053e000-7f6dd073d000 ---p 002b4000 fd:00 527730                     /usr/local/lib/libexiv2.so.13.0.0
```

```
7f6dd073d000-7f6dd0772000 r--p 002b3000 fd:00 527730                     /usr/local/lib/libexiv2.so.13.0.0
7f6dd0772000-7f6dd0776000 rw-p 002e8000 fd:00 527730                      /usr/local/lib/libexiv2.so.13.0.0
7f6dd0776000-7f6dd0790000 rw-p 00000000 00:00 0
7f6dd0790000-7f6dd07b1000 r-xp 00000000 fd:00 130827                      /usr/lib64/ld-2.20.so
7f6dd097f000-7f6dd0993000 rw-p 00000000 00:00 0
7f6dd09ae000-7f6dd09b1000 rw-p 00000000 00:00 0
7f6dd09b1000-7f6dd09b2000 r--p 00021000 fd:00 130827                     /usr/lib64/ld-2.20.so
7f6dd09b2000-7f6dd09b3000 rw-p 00022000 fd:00 130827                      /usr/lib64/ld-2.20.so
7f6dd09b3000-7f6dd09b4000 rw-p 00000000 00:00 0
7fff7d8ff000-7fff7d920000 rw-p 00000000 00:00 0                  [stack]
7fff7d9a8000-7fff7d9aa000 r--p 00000000 00:00 0                  [vvar]
7fff7d9aa000-7fff7d9ac000 r-xp 00000000 00:00 0                  [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0          [vsyscall]
Neúspěšně ukončen (SIGABRT) (core dumped [obraz paměti uložen])
```

History

#1 - 08 Apr 2015 12:38 - Martin Pučálka

Sorry, format is called WAV, of course.

#2 - 08 Apr 2015 13:38 - Robin Mills

- Subject changed from VAW file problem to WAV file problem

- Category set to video

- Status changed from New to Assigned

- Assignee set to Abhinav Badola

- Target version set to 0.26

Martin

Thanks for reporting this. I've assigned this to Abhinav to investigate in the first instance as he wrote the code involved. We have a GSoC (Google Summer of Code) student starting shortly and his project is to implement webm/webp support. http://dev.exiv2.org/issues/1048

Abhinav:
You can have a quick look at this. I can't assign it to Islam yet because he hasn't registered with us yet. I don't think his "slot" has been approved yet. His schedule is to join on April 27.

#3 - 12 Apr 2015 05:46 - Abhinav Badola

Yes, The bug is reproducible on my system as well.

The metadata of WAVE file is stored in container of RIFF class.
I will investigate into the bug and find a fix for it.

Thanks for reporting this bug, Martin.

Robin Mills wrote:

> Martin
>
> Thanks for reporting this. I've assigned this to Abhinav to investigate in the first instance as he wrote the code involved. We have a GSoC (Google Summer of Code) student starting shortly and his project is to implement webm/webp support. http://dev.exiv2.org/issues/1048
>
> Abhinav:
> You can have a quick look at this. I can't assign it to Islam yet because he hasn't registered with us yet. I don't think his "slot" has been approved yet. His schedule is to join on April 27.

#4 - 22 May 2015 09:26 - Jozef Mlich

The backtrace with debug info looks like this:

#0 0x00007ffff6d0ca98 in *GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:55*
#1 0x00007ffff6d0e72a in __GI_abort () at abort.c:89
*#2 0x00007ffff6d4fea2 in __libc_message (do_abort=do_abort@entry=2, fmt=fmt@entry=0x7ffff6e61a40 "*** Error in `%s': s: 0x%s ***\n") at ../sysdeps/posix/libc_fatal.c:175*
#3 0x00007ffff6d5753c in malloc_printerr (ptr=<optimized out>, str=0x7ffff6e61ae0 "free(): invalid next size (normal)", action=3) at malloc.c:4976
#4 _int_free (av=0x7ffff7092b20 <main_arena>, p=<optimized out>, have_lock=0) at malloc.c:3843
*#5 0x00007ffff6d5be9c in __GI_*libc_free (mem=<optimized out>) at malloc.c:2953

#6 0x00007ffff7a6428b in Exiv2::RiffVideo::infoTagsHandler() () from /usr/local/lib/libexiv2.so.13
#7 0x00007ffff7a697e5 in Exiv2::RiffVideo::decodeBlock() () from /usr/local/lib/libexiv2.so.13
#8 0x00007ffff7a69400 in Exiv2::RiffVideo::tagDecoder(Exiv2::DataBufx%x, unsigned long) () from /usr/local/lib/libexiv2.so.13
#9 0x00007ffff7a697e5 in Exiv2::RiffVideo::decodeBlock() () from /usr/local/lib/libexiv2.so.13
#10 0x00007ffff7a69b70 in Exiv2::RiffVideo::readMetadata() () from /usr/local/lib/libexiv2.so.13
#11 0x0000000000401867 in main ()

The debuging output
std::cout<<"|unprocessed|"<<buf.pData_;
says:
"|unprocessed|fact"

#5 - 22 May 2015 09:28 - Jozef Mlich

Jozef Mlich wrote:

> The backtrace with debug info looks like this:

#0 0x00007ffff6cf3a98 in *GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:55*
#1 0x00007ffff6cf572a in __GI_abort () at abort.c:89
*#2 0x00007ffff6d36ea2 in __libc_message (do_abort=do_abort@entry=2, fmt=fmt@entry=0x7ffff6e48a40 "*** Error in `%s': %s: 0x%s ***\n") at ../sysdeps/posix/libc_fatal.c:175*
#3 0x00007ffff6d3e53c in malloc_printerr (ptr=<optimized out>, str=0x7ffff6e48ae0 "free(): invalid next size (normal)", action=3) at malloc.c:4976
#4 _int_free (av=0x7ffff7079b20 <main_arena>, p=<optimized out>, have_lock=0) at malloc.c:3843
*#5 0x00007ffff6d42e9c in __GI_*libc_free (mem=<optimized out>) at malloc.c:2953
#6 0x00007ffff7a5ceaa in ~DataBuf (this=0x7fffffffdab0, __in_chrg=<optimized out>) at types.hpp:209
#7 Exiv2::RiffVideo::infoTagsHandler (this=0x6179a0) at riffvideo.cpp:891
#8 0x00007ffff7a60dd5 in Exiv2::RiffVideo::decodeBlock (this=this@entry=0x6179a0) at riffvideo.cpp:574
#9 0x00007ffff7a60a08 in Exiv2::RiffVideo::tagDecoder (this=this@entry=0x6179a0, buf=..., size=<optimized out>) at riffvideo.cpp:587
#10 0x00007ffff7a60dd5 in Exiv2::RiffVideo::decodeBlock (this=this@entry=0x6179a0) at riffvideo.cpp:574
#11 0x00007ffff7a61180 in Exiv2::RiffVideo::readMetadata (this=0x6179a0) at riffvideo.cpp:549
#12 0x0000000000401684 in main ()

> The debuging output
> std::cout<<"|unprocessed|"<<buf.pData_;
> says:
> "|unprocessed|fact"

#6 - 16 Sep 2016 07:00 - Robin Mills

- Status changed from Assigned to New

- Target version changed from 0.26 to 0.28

I'm going to defer this for v0.27. I'm also removing Abhinav as the assignee. I hope to have a team hangout in October 2016 to deal with assignments for v0.27.

#7 - 16 Sep 2016 07:01 - Robin Mills

- Assignee deleted (Abhinav Badola)

Files

FM00004.WAV	7.27 MB	08 Apr 2015	Martin Pučálka