CVE-2020-10812: Null pointer dereference in H5Fquery.c – HDF5 – 1.13.0

Null pointer dereference in H5Fquery.c – HDF5 – 1.13.0

Loginsoft-2020-1003

11 March, 2020

CVE Number

CVE-2020-10812

CWE

CWE – 476 : NULL Pointer Dereference

Product Details

HDF5 is a data model, library, and file format for storing and managing data. It supports an unlimited variety of data types and is designed for flexible and efficient I/O and for high volume and complex data. HDF5 is portable and is extensible, allowing applications to evolve in their use of HDF5. The HDF5 Technology suite includes tools and applications for managing, manipulating, viewing, and analyzing data in the HDF5 format.

URL: https://www.hdfgroup.org/downloads

Vulnerable Versions

1.13.0

Vulnerability Details

During our research we observed NULL pointer dereference in the function `H5F_get_nrefs()` located in `H5Fquery.c`. The same be triggered by sending a crafted file to the h5debug binary. It allows an attacker to cause Denial of Service.

SYNOPSIS

During our research on hdf5, when function H5VL__native_file_close() called in from H5VLnative_file.c to Handle the file close callback this calls another function H5F_get_nrefs() located in H5Fquery.c to Retrieve the file's 'nrefs' value, here in line FUNC_LEAVE_NOAPI(f->shared->nrefs) while fetching the value of f->shared->nrefs at this time the value of f->shared is pointing to null and it triggers the null pointer dereference.

vulnerable Source code

```
         H5F_get_nrefs(const H5F_t *f)
 {
     /* Use FUNC_ENTER_NOAPI_NOINIT_NOERR here to avoid performance issues */
     FUNC_ENTER_NOAPI_NOINIT_NOERR

     HDassert(f);
     HDassert(f->shared);

     FUNC_LEAVE_NOAPI(f->shared->nrefs)
 } /* end H5F_get_nrefs() */
```

Analysis

DEBUG:

GDB:

```
Starting program: /hdf5/build/bin/h5debug POC
Reading signature at address 0 (rel)
File Super Block...
File name (as opened):                             POC
File name (after resolving symlinks):              POC
File access flags                                  0x00000000
File open reference count:                         1
Address of super block:                            0 (abs)
Size of userblock:                                 0 bytes
Superblock version number:                         2
Free list version number:                          0
Root group symbol table entry version number:      0
Shared header version number:                      0
Size of file offsets (haddr_t type):               8 bytes
Size of file lengths (hsize_t type):               8 bytes
Symbol table leaf node 1/2 rank:                   4
Symbol table internal node 1/2 rank:               16
Indexed storage internal node 1/2 rank:            32
File status flags:                                 0x00
Superblock extension address:                      48 (rel)
Shared object header message table address:        UNDEF (rel)
Shared object header message version number:       0
Number of shared object header message indexes:    0
Address of driver information block:               UNDEF (rel)
Root group symbol table entry:
   Name offset into private heap:                  0
   Object header address:                          200
   Cache info type:                                Nothing Cached

Program received signal SIGSEGV, Segmentation fault.
[ Legend: Modified register | Code | Heap | Stack | String ]
──────────────────────────────────────────────────────────────────────────────────────────
registers ────
$rax   : 0x0
$rbx   : 0xffffffffffffffff
$rcx   : 0x0
$rdx   : 0x0
$rsp   : 0x00007fffffffd948  →  0x0000000000613bea  →   cmp eax, 0x1
$rbp   : 0x000000000078ed90  →  0x0000000000000000
$rsi   : 0xb000000000000008
$rdi   : 0x000000000078ed90  →  0x0000000000000000
$rip   : 0x00000000004883b4  →   mov eax, DWORD PTR [rax+0x1c]
$r8    : 0x1
$r9    : 0x5
$r10   : 0x0
$r11   : 0x00007fffffffdaa1  →  0x1d00706f745f542c (",T_top"?)
$r12   : 0x000000000074aa70  →  0x0000000000000001
$r13   : 0xb000000000000008
$r14   : 0x0
$r15   : 0x64
$eflags: [zero carry PARITY adjust sign trap INTERRUPT direction overflow RESUME virtualx86 identification]
$cs: 0x0033 $ss: 0x002b $ds: 0x0000 $es: 0x0000 $fs: 0x0000 $gs: 0x0000
──────────────────────────────────────────────────────────────────────────────────────────
stack ────
0x00007fffffffd948│+0x0000: 0x0000000000613bea  →   cmp eax, 0x1         ← $rsp
0x00007fffffffd950│+0x0008: 0x000000000074aa70  →  0x0000000000000001
0x00007fffffffd958│+0x0010: 0xffffffffffffffff
0x00007fffffffd960│+0x0018: 0x0000000000790fc0  →  0x0000000000000001
0x00007fffffffd968│+0x0020: 0x0000000000790f60  →  0x000000000078ed90  →  0x0000000000000000
0x00007fffffffd970│+0x0028: 0x0000000000000000
0x00007fffffffd978│+0x0030: 0x00000000005fae9f  →   test eax, eax
0x00007fffffffd980│+0x0038: 0x000000000074aa70  →  0x0000000000000001
──────────────────────────────────────────────────────────────────────────────────────────
code:x86:64 ────
     0x4883a2                  data16 nop WORD PTR cs:[rax+rax*1+0x0]
     0x4883ad                  nop    DWORD PTR [rax]
     0x4883b0  mov    rax, QWORD PTR [rdi+0x10]
 →   0x4883b4  mov    eax, DWORD PTR [rax+0x1c]
     0x4883b7  ret
     0x4883b8                  nop    DWORD PTR [rax+rax*1+0x0]
     0x4883c0  mov    rax, QWORD PTR [rdi+0x10]
     0x4883c4  mov    rax, QWORD PTR [rax+0x560]
     0x4883cb  ret
──────────────────────────────────────────────────────────────────────────────────────────
source:/h[...].c+601 ────
    596      FUNC_ENTER_NOAPI_NOINIT_NOERR
    597
    598      HDassert(f);
    599      HDassert(f->shared);
    600
 →  601      FUNC_LEAVE_NOAPI(f->shared->nrefs)
    602  } /* end H5F_get_nrefs() */
    603
    604
    605  /*-------------------------------------------------------------------------
    606   * Function: H5F_rdcc_nslots
──────────────────────────────────────────────────────────────────────────────────────────
threads ────
[#0] Id 1, Name: "h5debug", stopped, reason: SIGSEGV
──────────────────────────────────────────────────────────────────────────────────────────
trace ────
[#0] 0x4883b4 → H5F_get_nrefs(f=0x78ed90)
[#1] 0x613bea → H5VL__native_file_close(file=0x78ed90, dxpl_id=, req=)
[#2] 0x5fae9f → H5VL__file_close(obj=, dxpl_id=0xb000000000000008, req=0x0, cls=)
[#3] 0x603245 → H5VL_file_close(vol_obj=0x790f60, dxpl_id=0xb000000000000008, req=0x0)
[#4] 0x47742d → H5F__close_cb(file_vol_obj=0x790f60)
[#5] 0x4d7aef → H5I__clear_type_cb(_id=0x790f80, key=, _udata=0x7fffffffda50)
[#6] 0x579083 → H5SL_try_free_safe(slist=0x78d270, op=0x4d7ab0 , op_data=0x7fffffffda50)
[#7] 0x4d86dd → H5I_clear_type(type=H5I_FILE, force=0x0, app_ref=0x0)
[#8] 0x47760c → H5F_term_package()
[#9] 0x403f77 → H5_term_library()
──────────────────────────────────────────────────────────────────────────────────────────
0x00000000004883b4 in H5F_get_nrefs (f=f@entry=0x78ed90) at /hdf5/src/H5Fquery.c:601
601         FUNC_LEAVE_NOAPI(f->shared->nrefs)
gef➤  bt
#0  0x00000000004883b4 in H5F_get_nrefs (f=f@entry=0x78ed90) at /hdf5/src/H5Fquery.c:601
#1  0x0000000000613bea in H5VL__native_file_close (file=0x78ed90, dxpl_id=, req=) at
/hdf5/src/H5VLnative_file.c:869
#2  0x00000000005fae9f in H5VL__file_close (obj=, dxpl_id=dxpl_id@entry=0xb000000000000008, req=req@entry=0x0,
cls=) at /hdf5/src/H5VLcallback.c:3945
#3  0x0000000000603245 in H5VL_file_close (vol_obj=vol_obj@entry=0x790f60, dxpl_id=0xb000000000000008,
req=req@entry=0x0) at /hdf5/src/H5VLcallback.c:3977
#4  0x000000000047742d in H5F__close_cb (file_vol_obj=0x790f60) at /hdf5/src/H5F.c:242
#5  0x00000000004d7aef in H5I__clear_type_cb (_id=0x790f80, key=, _udata=0x7fffffffda50) at /hdf5/src/H5I.c:611
#6  0x0000000000579083 in H5SL_try_free_safe (slist=0x78d270, op=op@entry=0x4d7ab0 ,
op_data=op_data@entry=0x7fffffffda50) at /hdf5/src/H5SL.c:2369
#7  0x00000000004d86dd in H5I_clear_type (type=type@entry=H5I_FILE, force=force@entry=0x0,
app_ref=app_ref@entry=0x0) at /hdf5/src/H5I.c:571
#8  0x000000000047760c in H5F_term_package () at /hdf5/src/H5F.c:194
#9  0x0000000000403f77 in H5_term_library () at /hdf5/src/H5.c:323
#10 0x00007ffff7485041 in __run_exit_handlers (status=0x0, listp=0x7ffff782d718 ,
run_list_atexit=run_list_atexit@entry=0x1, run_dtors=run_dtors@entry=0x1) at exit.c:108
#11 0x00007ffff748513a in __GI_exit (status=) at exit.c:139
#12 0x00007ffff7463b9e in __libc_start_main (main=0x402720 , argc=0x2, argv=0x7fffffffe018, init=, fini=,
rtld_fini=, stack_end=0x7fffffffe008) at ../csu/libc-start.c:344
#13 0x000000000040370a in _start ()
gef➤  i r
rax            0x0      0x0
rbx            0xffffffffffffffff       0xffffffffffffffff
rcx            0x0      0x0
rdx            0x0      0x0
rsi            0xb000000000000008       0xb000000000000008
rdi            0x78ed90 0x78ed90
rbp            0x78ed90 0x78ed90
rsp            0x7fffffffd948   0x7fffffffd948
r8             0x1      0x1
r9             0x5      0x5
r10            0x0      0x0
r11            0x7fffffffdaa1   0x7fffffffdaa1
r12            0x74aa70 0x74aa70
r13            0xb000000000000008       0xb000000000000008
r14            0x0      0x0
```

```
rip            0x4883b4 0x4883b4
eflags         0x10206  [ PF IF RF ]
cs             0x33     0x33
ss             0x2b     0x2b
ds             0x0      0x0
es             0x0      0x0
fs             0x0      0x0
gs             0x0      0x0
gef➤  p f->shared->nrefs
Cannot access memory at address 0x1c
gef➤  p f->shared
$1 = (H5F_shared_t *) 0x0
gef➤  ptype f
type = const struct H5F_t {
    char *open_name;
    char *actual_name;
    H5F_shared_t *shared;
    H5VL_object_t *vol_obj;
    unsigned int nopen_objs;
    H5FO_t *obj_count;
    hbool_t id_exists;
    hbool_t closing;
    struct H5F_t *parent;
    unsigned int nmounts;
} *
```

ASAN Output:

```
Reading signature at address 0 (rel)
File Super Block...
File name (as opened):                             POC
File name (after resolving symlinks):              POC
File access flags                                  0x00000000
File open reference count:                         1
Address of super block:                            0 (abs)
Size of userblock:                                 0 bytes
Superblock version number:                         2
Free list version number:                          0
Root group symbol table entry version number:      0
Shared header version number:                      0
Size of file offsets (haddr_t type):               8 bytes
Size of file lengths (hsize_t type):               8 bytes
Symbol table leaf node 1/2 rank:                   4
Symbol table internal node 1/2 rank:               16
Indexed storage internal node 1/2 rank:            32
File status flags:                                 0x00
Superblock extension address:                      48 (rel)
Shared object header message table address:        UNDEF (rel)
Shared object header message version number:       0
Number of shared object header message indexes:    0
Address of driver information block:               UNDEF (rel)
Root group symbol table entry:
   Name offset into private heap:                  0
   Object header address:                          200
   Cache info type:                                Nothing Cached
ASAN:DEADLYSIGNAL
=================================================================
==20845==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000001c (pc 0x55a9417f4aff bp 0x6070000001e0 sp
0x7ffe5115db20 T0)
==20845==The signal is caused by a READ memory access.
==20845==Hint: address points to the zero page.
    #0 0x55a9417f4afe in H5F_get_nrefs /hdf5/src/H5Fquery.c:601
    #1 0x55a941c12240 in H5VL__native_file_close /hdf5/src/H5VLnative_file.c:869
    #2 0x55a941bd67ac in H5VL__file_close /hdf5/src/H5VLcallback.c:3945
    #3 0x55a941be8bef in H5VL_file_close /hdf5/src/H5VLcallback.c:3977
    #4 0x55a9417c7353 in H5F__close_cb /hdf5/src/H5F.c:242
    #5 0x55a9418d14ea in H5I__clear_type_cb /hdf5/src/H5I.c:611
    #6 0x55a941a8fad2 in H5SL_try_free_safe /hdf5/src/H5SL.c:2369
    #7 0x55a9418d3086 in H5I_clear_type /hdf5/src/H5I.c:571
    #8 0x55a9417c768b in H5F_term_package /hdf5/src/H5F.c:194
    #9 0x55a94168ce4e in H5_term_library /hdf5/src/H5.c:323
    #10 0x7f9de98ba040  (/lib/x86_64-linux-gnu/libc.so.6+0x43040)
    #11 0x7f9de98ba139 in exit (/lib/x86_64-linux-gnu/libc.so.6+0x43139)
    #12 0x7f9de9898b9d in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b9d)
    #13 0x55a94168c049 in _start (/hdf5/build1/bin/h5debug+0x148049)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /hdf5/src/H5Fquery.c:601 in H5F_get_nrefs
==20845==ABORTING
```

Proof of Concept

`./h5debug $POC`

Vendor Disclosure: 2020-3-10

Credit

Discovered by ACE Team – Loginsoft

Let us know how we can help you

CONTACT

US Office
4437 Brookfield Corporate Drive, Suite 101
Chantilly, VA USA 20151.
+1 703 956 7410

Canada Office
7-7003 Steeles Ave W, Toronto,
ON M9W 0A2, Canada.

India Office
1-63-5-8B, Kavuri Hills, Jubilee Hills,
Hyderabad-500033.

Privacy and Disclosure Policy