CVE-2020-10811: Heap buffer overflow in H5Olayout.c – HDF5 – 1.13.0

Heap buffer overflow in H5Olayout.c – HDF5 – 1.13.0

Loginsoft-2020-1004

11 March, 2020

CVE Number

CVE-2020-10811

CWE

CWE – 122 : Heap-based Buffer Overflow

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 Heap overflow in the function `H5O__layout_decode()` located in `H5Olayout.c`. The same be triggered by sending a crafted file to the h5dump binary. It allows an attacker to cause Denial of Service.

SYNOPSIS

In progress.

vulnerable Source code

```
       187              if(mesg->type == H5D_COMPACT) {
    188                UINT32DECODE(p, mesg->storage.u.compact.size);
    189                if(mesg->storage.u.compact.size > 0) {
    190                    if(NULL == (mesg->storage.u.compact.buf = H5MM_malloc(mesg->storage.u.compact.size)))
    191                        HGOTO_ERROR(H5E_RESOURCE, H5E_NOSPACE, NULL, "memory allocation failed for compact
data buffer")
  → 192                             H5MM_memcpy(mesg->storage.u.compact.buf, p, mesg->storage.u.compact.size);
    193                    p += mesg->storage.u.compact.size;
    194                } /* end if */
    195            } /* end if */
```

Analysis

DEBUG:

GDB:

```
Starting program: /hdf5/build1/bin/h5dump -r -d BAG_root/metadata $POC

Program received signal SIGSEGV, Segmentation fault.
 [ Legend: Modified register | Code | Heap | Stack | String ]

────────────────────────────────────────────────────────────────────────────────────────────────────────
registers ────
 $rax   : 0x00007ffff7e16010  →  0x0000000000000000
 $rbx   : 0x0000000001255370  →  0x0000000100000000
 $rcx   : 0x00007ffff7e16010  →  0x0000000000000000
 $rdx   : 0x140001
$rsp   : 0x00007fffffffd088  →  0x0000000000823058  →   mov r9, QWORD PTR [rbx+0x788]
 $rbp   : 0x0
$rsi   : 0x00000000012541e8  →  "scaleoffset"
 $rdi   : 0x00007ffff7e16010  →  0x0000000000000000
 $rip   : 0x00007ffff75d0cf4  →   vmovdqu ymm8, YMMWORD PTR [rsi+rdx*1-0x20]
 $r8    : 0xffffffff
$r9    : 0x0
$r10   : 0x22
$r11   : 0x246
$r12   : 0x0
$r13   : 0x00000000012541e7  →  0x666f656c61637300
 $r14   : 0x00000000012541e8  →  "scaleoffset"
 $r15   : 0x1
 $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 ────
 0x00007fffffffd088│+0x0000: 0x0000000000823058  →   mov r9, QWORD PTR [rbx+0x788]           ← $rsp
 0x00007fffffffd090│+0x0008: 0x0000000000000000
 0x00007fffffffd098│+0x0010: 0x0000000000564ee2  →   mov rax, QWORD PTR [rsp+0x10]
 0x00007fffffffd0a0│+0x0018: 0x00000000004cac00  →   and al, 0x10
 0x00007fffffffd0a8│+0x0020: 0x00000000012541e8  →  "scaleoffset"
 0x00007fffffffd0b0│+0x0028: 0x0000000000000000
 0x00007fffffffd0b8│+0x0030: 0x00000000008333ae  →   mov rax, QWORD PTR [rsp+0x10]
 0x00007fffffffd0c0│+0x0038: 0x0000000000000008

────────────────────────────────────────────────────────────────────────────────────────────────────────
code:x86:64 ────
    0x7ffff75d0ce4  vmovdqu ymm5, YMMWORD PTR es:[rsi+0x20]
    0x7ffff75d0cea  vmovdqu ymm6, YMMWORD PTR [rsi+0x40]
    0x7ffff75d0cef  vmovdqu ymm7, YMMWORD PTR [rsi+0x60]
  → 0x7ffff75d0cf4  vmovdqu ymm8, YMMWORD PTR [rsi+rdx*1-0x20]
    0x7ffff75d0cfa  lea    r11, [rdi+rdx*1-0x20]
    0x7ffff75d0cff  lea    rcx, [rsi+rdx*1-0x20]
    0x7ffff75d0d04  mov    r9, r11
    0x7ffff75d0d07  mov    r8, r11
    0x7ffff75d0d0a  and    r8, 0x1f

────────────────────────────────────────────────────────────────────────────────────────────────────────
threads ────
 [#0] Id 1, Name: "h5dump", stopped, reason: SIGSEGV

────────────────────────────────────────────────────────────────────────────────────────────────────────
trace ────
 [#0] 0x7ffff75d0cf4 → __memmove_avx_unaligned_erms()
 [#1] 0x823058 → H5O__layout_decode(f=, open_oh=, mesg_flags=, ioflags=, p_size=, p=)
 [#2] 0x83371f → H5O_msg_read_oh(f=0x123aa10, oh=0x1253f90, type_id=0x8, mesg=0x123ff28)
 [#3] 0x833f25 → H5O_msg_read(loc=0x123fdd0, type_id=0x8, mesg=0x123ff28)
 [#4] 0x5aabe8 → H5D__layout_oh_read(dataset=0x123fdd0, dapl_id=0xb00000000000007, plist=0x1241410)
 [#5] 0x5972da → H5D__open_oid(dapl_id=0xb00000000000007, dataset=0x123fdd0)
 [#6] 0x5972da → H5D_open(loc=0x7fffffffd300, dapl_id=0xb00000000000007)
 [#7] 0x5997d3 → H5D__open_name(loc=0x7fffffffd380, name=0x124c530 "/Scale_offset_float_data_le",
dapl_id=0xb00000000000007)
 [#8] 0xed2942 → H5VL__native_dataset_open(obj=, loc_params=0x7fffffffd410, name=0x124c530
"/Scale_offset_float_data_le", dapl_id=0xb00000000000007, dxpl_id=0xb00000000000008, req=)
 [#9] 0xe8ff52 → H5VL__dataset_open(cls=0x12045c0, req=0x0, dxpl_id=0xb00000000000008, dapl_id=0xb00000000000007,
name=0x124c530 "/Scale_offset_float_data_le", loc_params=0x7fffffffd410, obj=)

────────────────────────────────────────────────────────────────────────────────────────────────────────
 __memmove_avx_unaligned_erms () at ../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:427
 427       ../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S: No such file or directory.



gef➤  i r
 rax            0x7ffff7e16010         0x7ffff7e16010
 rbx            0x1255370    0x1255370
 rcx            0x7ffff7e16010         0x7ffff7e16010
 rdx            0x140001     0x140001
 rsi            0x12541e8     0x12541e8
 rdi            0x7ffff7e16010          0x7ffff7e16010
 rbp            0x0  0x0
 rsp            0x7fffffffd088           0x7fffffffd088
 r8             0xffffffff       0xffffffff
 r9             0x0   0x0
 r10            0x22            0x22
 r11            0x246           0x246
 r12            0x0  0x0
 r13            0x12541e7    0x12541e7
 r14            0x12541e8    0x12541e8
 r15            0x1  0x1
 rip            0x7ffff75d0cf4          0x7ffff75d0cf4
 eflags         0x10216       [ PF AF IF RF ]
 cs             0x33 0x33
 ss             0x2b  0x2b
 ds             0x0   0x0
 es             0x0   0x0
 fs             0x0   0x0
 gs             0x0   0x0
 gef➤  bt
 #0  __memmove_avx_unaligned_erms () at ../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:427
 #1  0x0000000000823058 in H5O__layout_decode (f=, open_oh=, mesg_flags=, ioflags=, p_size=, p=) at
/hdf5/src/H5Olayout.c:192
 #2  0x000000000083371f in H5O_msg_read_oh (f=0x123aa10, oh=oh@entry=0x1253f90, type_id=type_id@entry=0x8,
mesg=mesg@entry=0x123ff28) at /hdf5/src/H5Omessage.c:541
 #3  0x0000000000833f25 in H5O_msg_read (loc=loc@entry=0x123fdd0, type_id=type_id@entry=0x8, mesg=0x123ff28) at
/hdf5/src/H5Omessage.c:480
 #4  0x00000000005aabe8 in H5D__layout_oh_read (dataset=dataset@entry=0x123fdd0,
dapl_id=dapl_id@entry=0xb00000000000007, plist=plist@entry=0x1241410) at /hdf5/src/H5Dlayout.c:636
 #5  0x00000000005972da in H5D__open_oid (dapl_id=0xb00000000000007, dataset=0x123fdd0) at /hdf5/src/H5Dint.c:1771
 #6  H5D_open (loc=loc@entry=0x7fffffffd300, dapl_id=dapl_id@entry=0xb00000000000007) at /hdf5/src/H5Dint.c:1558
 #7  0x00000000005997d3 in H5D__open_name (loc=loc@entry=0x7fffffffd380, name=name@entry=0x124c530
"/Scale_offset_float_data_le", dapl_id=dapl_id@entry=0xb00000000000007) at /hdf5/src/H5Dint.c:1492
 #8  0x0000000000ed2942 in H5VL__native_dataset_open (obj=, loc_params=loc_params@entry=0x7fffffffd410,
name=name@entry=0x124c530 "/Scale_offset_float_data_le", dapl_id=dapl_id@entry=0xb00000000000007,
dxpl_id=dxpl_id@entry=0xb00000000000008, req=) at /hdf5/src/H5VLnative_dataset.c:124
 #9  0x0000000000e8ff52 in H5VL__dataset_open (cls=0x12045c0, req=0x0, dxpl_id=0xb00000000000008,
dapl_id=0xb00000000000007, name=0x124c530 "/Scale_offset_float_data_le", loc_params=0x7fffffffd410, obj=) at
/hdf5/src/H5VLcallback.c:1941
 #10 H5VL_dataset_open (vol_obj=vol_obj@entry=0x123cd30, loc_params=loc_params@entry=0x7fffffffd410,
name=name@entry=0x124c530 "/Scale_offset_float_data_le", dapl_id=0xb00000000000007, dxpl_id=0xb00000000000008,
req=req@entry=0x0) at /hdf5/src/H5VLcallback.c:1974
 #11 0x000000000056f94b in H5Dopen2 (loc_id=0x100000000000000, name=name@entry=0x124c530
"/Scale_offset_float_data_le", dapl_id=, dapl_id@entry=0x0) at /hdf5/src/H5D.c:295
 #12 0x000000000048cc05 in find_objs_cb (name=0x124c530 "/Scale_offset_float_data_le", oinfo=0x7fffffffd530,
already_seen=, op_data=) at /hdf5/tools/lib/h5tools_utils.c:741
 #13 0x0000000000490904 in traverse_cb (loc_id=, path=, linfo=, _udata=) at /hdf5/tools/lib/h5trav.c:224
 #14 0x00000000006c673d in H5G_visit_cb (lnk=0x7fffffffd6f0, _udata=0x7fffffffd990) at /hdf5/src/H5Gint.c:917
 #15 0x00000000006df009 in H5G__node_iterate (f=0x123aa10, _lt_key=, addr=0x56d8, _rt_key=, _udata=0x7fffffffd820)
at /hdf5/src/H5Gnode.c:1001
 #16 0x00000000010174cf in H5B__iterate_helper (udata=, op=, addr=, type=, f=) at /hdf5/src/H5B.c:1166
 #17 H5B_iterate (f=0x123aa10, type=0x11ee6e0 , addr=0x88, op=0x6deb90 , udata=udata@entry=0x7fffffffd820) at
/hdf5/src/H5B.c:1211
 #18 0x00000000006eec49 in H5G__stab_iterate (oloc=oloc@entry=0x123db08, order=order@entry=H5_ITER_INC,
skip=skip@entry=0x0, last_lnk=last_lnk@entry=0x0, op=op@entry=0x6c64b0 , op_data=op_data@entry=0x7fffffffd990) at
/hdf5/src/H5Gstab.c:556
 #19 0x00000000006e5c29 in H5G__obj_iterate (grp_oloc=grp_oloc@entry=0x123db08,
idx_type=idx_type@entry=H5_INDEX_NAME, order=order@entry=H5_ITER_INC, skip=skip@entry=0x0,
last_lnk=last_lnk@entry=0x0, op=op@entry=0x6c64b0 , op_data=0x7fffffffd990) at /hdf5/src/H5Gobj.c:696
 #20 0x00000000006cb39b in H5G_visit (loc=loc@entry=0x7fffffffda30, group_name=,
idx_type=idx_type@entry=H5_INDEX_NAME, order=order@entry=H5_ITER_INC, op=op@entry=0x4902d0 , op_data=) at
```

```
 #21 0x0000000000ee4ddc in H5VL__native_link_specific (obj=, loc_params=loc_params@entry=0x7fffffffdbe0,
specific_type=specific_type@entry=H5VL_LINK_ITER, dxpl_id=dxpl_id@entry=0xb00000000000008, req=,
arguments=arguments@entry=0x7fffffffda98) at /hdf5/src/H5VLnative_link.c:371
 #22 0x0000000000ea818f in H5VL__link_specific (cls=, arguments=0x7fffffffda98, req=0x0,
dxpl_id=0xb00000000000008, specific_type=H5VL_LINK_ITER, loc_params=0x7fffffffdbe0, obj=) at
/hdf5/src/H5VLcallback.c:5161
 #23 H5VL_link_specific (vol_obj=vol_obj@entry=0x123cd30, loc_params=loc_params@entry=0x7fffffffdbe0,
specific_type=specific_type@entry=H5VL_LINK_ITER, dxpl_id=0xb00000000000008, req=req@entry=0x0) at
/hdf5/src/H5VLcallback.c:5198
 #24 0x000000000078631a in H5Lvisit_by_name2 (loc_id=loc_id@entry=0x100000000000000,
group_name=group_name@entry=0x110d24d "/", idx_type=H5_INDEX_NAME, order=H5_ITER_INC, op=op@entry=0x4902d0 ,
op_data=op_data@entry=0x7fffffffdcb0, lapl_id=) at /hdf5/src/H5L.c:1544
 #25 0x00000000004950ed in traverse (fields=0x1, visitor=0x7fffffffdc70, recurse=0x1, visit_start=,
grp_name=0x110d24d "/", file_id=0x100000000000000) at /hdf5/tools/lib/h5trav.c:295
 #26 h5trav_visit (fid=fid@entry=0x100000000000000, grp_name=grp_name@entry=0x110d24d "/",
visit_start=visit_start@entry=0x1, recurse=recurse@entry=0x1, visit_obj=visit_obj@entry=0x48c790 ,
visit_lnk=visit_lnk@entry=0x0, udata=0x7fffffffddc0, fields=0x1) at /hdf5/tools/lib/h5trav.c:1079
 #27 0x000000000048d1ab in init_objs (fid=fid@entry=0x100000000000000, info=info@entry=0x7fffffffddc0,
group_table=0x123d2a0, dset_table=0x123d2a8, type_table=0x123d2b0) at /hdf5/tools/lib/h5tools_utils.c:816
 #28 0x0000000000410245 in table_list_add (oid=oid@entry=0x100000000000000, file_no=0x1) at
/hdf5/tools/src/h5dump/h5dump.c:429
 #29 0x0000000000407699 in main (argc=, argv=0x7fffffffdfc8) at /hdf5/tools/src/h5dump/h5dump.c:1577
gef➤  p/d mesg->storage.u.compact.size
 $1 = 1310721
 gef➤  p/d mesg->storage.u.compact.buf
 $2 = 140737352130576
gef➤  p mesg->storage
 $2 = {
   type = H5D_COMPACT,
  u = {
     contig = {
       addr = 0x0,
      size = 0x140001
     },
    chunk = {
       idx_type = H5D_CHUNK_IDX_BTREE,
      idx_addr = 0x140001,
      ops = 0x7ffff33be800,
      u = {
         btree = {
           dset_ohdr_addr = 0x0,
          shared = 0x0
         },
        btree2 = {
           dset_ohdr_addr = 0x0,
          bt2 = 0x0
         },
        earray = {
           dset_ohdr_addr = 0x0,
          ea = 0x0
         },
        farray = {
           dset_ohdr_addr = 0x0,
          fa = 0x0
         },
        single = {
           nbytes = 0x0,
          filter_mask = 0x0
         }
       }
     },
    compact = {
       dirty = 0x0,
      size = 0x140001,
      buf = 0x7ffff33be800
     },
    virt = {
       serial_list_hobjid = {
         addr = 0x0,
        idx = 0x140001
       },
      list_nused = 0x7ffff33be800,
      list = 0x0,
      list_nalloc = 0x0,
      min_dims = {0x0 },
      view = H5D_VDS_FIRST_MISSING,
      printf_gap = 0x0,
      source_fapl = 0x0,
      source_dapl = 0x0,
      init = 0x0
     }
   }
 }
```

ASAN Output:

```
 ==20317==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x612000029cf8 at pc 0x7f012c002733 bp
0x7ffdd6a32b60 sp 0x7ffdd6a32308
 READ of size 1310721 at 0x612000029cf8 thread T0
     #0 0x7f012c002732  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x79732)
     #1 0x555b9c28b6ae in H5O__layout_decode hdf5/src/H5Olayout.c:192
     #2 0x555b9c296486 in H5O_msg_read_oh /hdf5/src/H5Omessage.c:541
     #3 0x555b9c296d5f in H5O_msg_read /hdf5/src/H5Omessage.c:480
     #4 0x555b9c09f84a in H5D__layout_oh_read /hdf5/src/H5Dlayout.c:636
     #5 0x555b9c08f83f in H5D__open_oid /hdf5/src/H5Dint.c:1771
     #6 0x555b9c08f83f in H5D_open /hdf5/src/H5Dint.c:1558
     #7 0x555b9c0919cc in H5D__open_name /hdf5/src/H5Dint.c:1492
     #8 0x555b9c5606ec in H5VL__native_dataset_open /hdf5/src/H5VLnative_dataset.c:124
     #9 0x555b9c52cf1b in H5VL__dataset_open /hdf5/src/H5VLcallback.c:1941
     #10 0x555b9c5392a6 in H5VL_dataset_open /hdf5/src/H5VLcallback.c:1974
     #11 0x555b9c07010b in H5Dopen2 /hdf5/src/H5D.c:295
     #12 0x555b9bfc53c5 in find_objs_cb /hdf5/tools/lib/h5tools_utils.c:741
     #13 0x555b9bfc8ab6 in traverse_cb /hdf5/tools/lib/h5trav.c:224
     #14 0x555b9c172439 in H5G_visit_cb /hdf5/src/H5Gint.c:917
     #15 0x555b9c187739 in H5G__node_iterate /hdf5/src/H5Gnode.c:1001
     #16 0x555b9c5c5c48 in H5B__iterate_helper /hdf5/src/H5B.c:1166
     #17 0x555b9c5c9105 in H5B_iterate /hdf5/src/H5B.c:1211
     #18 0x555b9c196289 in H5G__stab_iterate /hdf5/src/H5Gstab.c:556
     #19 0x555b9c18ee36 in H5G__obj_iterate /hdf5/src/H5Gobj.c:696
     #20 0x555b9c17742a in H5G_visit /hdf5/src/H5Gint.c:1143
     #21 0x555b9c56f065 in H5VL__native_link_specific /hdf5/src/H5VLnative_link.c:371
     #22 0x555b9c5303ce in H5VL__link_specific /hdf5/src/H5VLcallback.c:5161
     #23 0x555b9c5462c5 in H5VL_link_specific /hdf5/src/H5VLcallback.c:5198
     #24 0x555b9c20cb3f in H5Lvisit_by_name2 /hdf5/src/H5L.c:1544
     #25 0x555b9bfc727f in traverse /hdf5/tools/lib/h5trav.c:295
     #26 0x555b9bfcaa1f in h5trav_visit /hdf5/tools/lib/h5trav.c:1079
     #27 0x555b9bfc567d in init_objs /hdf5/tools/lib/h5tools_utils.c:816
     #28 0x555b9bf76ea8 in table_list_add /hdf5/tools/src/h5dump/h5dump.c:429
     #29 0x555b9bf6f3d7 in main /hdf5/tools/src/h5dump/h5dump.c:1577
     #30 0x7f012b617b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
     #31 0x555b9bf74339 in _start (/hdf5/build/bin/h5dump+0x15f339)

0x612000029cf8 is located 0 bytes to the right of 312-byte region [0x612000029bc0,0x612000029cf8)
 allocated by thread T0 here:
     #0 0x7f012c067b50 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb50)
     #1 0x555b9c15346c in H5FL_malloc /hdf5/src/H5FL.c:243

SUMMARY: AddressSanitizer: heap-buffer-overflow (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x79732)
Shadow bytes around the buggy address:
   0x0c247fffd340: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
   0x0c247fffd350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   0x0c247fffd360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
   0x0c247fffd370: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
   0x0c247fffd380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 =>0x0c247fffd390: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[fa]
   0x0c247fffd3a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c247fffd3b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c247fffd3c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c247fffd3d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c247fffd3e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 Shadow byte legend (one shadow byte represents 8 application bytes):
   Addressable:           00
   Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
   Freed heap region:       fd
   Stack left redzone:      f1
   Stack mid redzone:       f2
   Stack right redzone:     f3
   Stack after return:      f5
   Stack use after scope:   f8
   Global redzone:          f9
   Global init order:       f6
   Poisoned by user:        f7
   Container overflow:      fc
   Array cookie:            ac
   Intra object redzone:    bb
   ASan internal:           fe
   Left alloca redzone:     ca
   Right alloca redzone:    cb
```

Proof of Concept

```
./h5dump -r -d BAG_root/metadata $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