CVE-2020-10810: Null pointer dereference in H5AC.c – HDF5 – 1.13.0

Null pointer dereference in H5AC.c – HDF5 – 1.13.0

Loginsoft-2020-1005

11 March, 2020

CVE Number

CVE-2020-10810

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 `H5AC_unpin_entry()` located in `H5AC.c`. The same be triggered by sending a crafted file to the h5clear binary. It allows an attacker to cause Denial of Service.

SYNOPSIS

During our research on hdf5, When function H5F__dest() to flushe the cache located in H5Fint.c calls another function H5AC_unpin_entry() to Unpin a cache entry located in H5AC.c, here before calling function H5C_log_write_unpin_entry_msg() for generating log message in line if(cache_ptr->log_info->logging) it is trying to dereference cache_ptr() pointer which is null and it triggers the null pointer dereference.

vulnerable Source code

```
1418       /* If currently logging, generate a message */
→ 1419               if(cache_ptr->log_info->logging)
  1420           if(H5C_log_write_unpin_entry_msg(cache_ptr, entry_ptr, ret_value) < 0)
  1421               HDONE_ERROR(H5E_CACHE, H5E_LOGGING, FAIL, "unable to emit log message")
  1422
 1423       FUNC_LEAVE_NOAPI(ret_value)
  1424   } /* H5AC_unpin_entry() */
```

Analysis

DEBUG:

GDB:

```
Starting program: /hdf5/build/bin/h5clear -s -m POC

Program received signal SIGSEGV, Segmentation fault.
 [ Legend: Modified register | Code | Heap | Stack | String ]
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
registers ────
 $rax   : 0x0
$rbx   : 0x0
$rcx   : 0xd0000000000003c
$rdx   : 0x000055555634b010  →  0x0000010000010001
 $rsp   : 0x00007fffffffdbd0  →  0x0000000000000000
 $rbp   : 0x000055555638fc40  →  0x0000000000000000
 $rsi   : 0x000055555626b2ea  →  "can't unpin entry"
 $rdi   : 0x0
$rip   : 0x000055555555f425c  →   mov rdi, QWORD PTR [rbx+0x8]
 $r8    : 0x000055555634a138  →  0x0000555556391840  →  "Can't unpin entry from client"
 $r9    : 0x72746e65206e6970 ("pin entr"?)
 $r10   : 0x000055555634b010  →  0x0000010000010001
 $r11   : 0x0
$r12   : 0xffffffff
$r13   : 0x0
$r14   : 0x000055555638ea10  →  0x0800000000000000
 $r15   : 0x000055555638e8e0  →  0x000055555563 8f8f0  →  "POC"
 $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 ────
 0x00007fffffffdbd0|+0x0000: 0x0000000000000000       ← $rsp
 0x00007fffffffdbd8|+0x0008: 0x000055555638e8e0  →  0x000055555638f8f0  →
"h5clear_fuzz/id:000033,sig:11,src:000169,op:flip1,[...]"
 0x00007fffffffdbe0|+0x0010: 0x0000000000000000
 0x00007fffffffdbe8|+0x0018: 0x0000555556346ac8  →  0x0000000000000001
 0x00007fffffffdbf0|+0x0020: 0x0000000000000000
 0x00007fffffffdbf8|+0x0028: 0x00005555557601f1  →   test eax, eax
 0x00007fffffffdc00|+0x0030: 0x000055555638e5c0  →  0x000055555635 8350  →  0x0000555556354230  →
0x0000000000000000
 0x00007fffffffdc08|+0x0038: 0x00005555563413f8  →  0x0c00000000000000
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
code:x86:64 ────
    0x5555555f424b  mov    rcx, QWORD PTR [rsp+0x8]
    0x5555555f4250  mov    rdx, QWORD PTR [rsp]
    0x5555555f4254  lea    rsp, [rsp+0x98]
  → 0x5555555f425c  mov    rdi, QWORD PTR [rbx+0x8]
    0x5555555f4260  cmp    BYTE PTR [rdi+0x1], 0x0
    0x5555555f4264  je     0x5555555f4080
    0x5555555f426a  xchg   ax, ax
    0x5555555f426c  lea    rsp, [rsp-0x98]
    0x5555555f4274  mov    QWORD PTR [rsp], rdx
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
source:/h[...].c+1419 ────
    1414       if(H5C_unpin_entry(thing) log_info->logging)
    1420           if(H5C_log_write_unpin_entry_msg(cache_ptr, entry_ptr, ret_value) < 0)
    1421               HDONE_ERROR(H5E_CACHE, H5E_LOGGING, FAIL, "unable to emit log message")
    1422
   1423       FUNC_LEAVE_NOAPI(ret_value)
    1424   } /* H5AC_unpin_entry() */
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
threads ────
 [#0] Id 1, Name: "h5clear", stopped, reason: SIGSEGV
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
trace ────
 [#0] 0x5555555f425c → H5AC_unpin_entry(thing=0x55555638fc40)
 [#1] 0x55555557601f1 → H5F__dest(f=0x55555638e8e0, flush=0x0)
 [#2] 0x55555576ba43 → H5F_open(name=, flags=, fcpl_id=, fapl_id=)
 [#3] 0x555556 01a78b → H5VL__native_file_open(name=, flags=, fapl_id=, dxpl_id=, req=)
 [#4] 0x555555fdb1b9 → H5VL__file_open(cls=, req=0x0, dxpl_id=0xb00000000000008, fapl_id=0xb00000000000014,
flags=0x1, name=0x55555638d2d0 "h5clear_fuzz/id:000033,sig:11,src:000169,op:flip1,pos:73")
 [#5] 0x555555fdb1b9 → H5VL_file_open(connector_prop=0x7fffffffdd40, name=0x55555638d2d0
"h5clear_fuzz/id:000033,sig:11,src:000169,op:flip1,pos:73", flags=0x1, fapl_id=0xb00000000000014,
dxpl_id=0xb00000000000008, req=0x0)
 [#6] 0x5555557 45908 → H5Fopen(filename=0x55555638d2d0 "h5clear_fuzz/id:000033,sig:11,src:000169,op:flip1,pos:73",
flags=0x1, fapl_id=)
 [#7] 0x5555555683d8 → h5tools_fopen(fname=0x55555638d2d0
"h5clear_fuzz/id:000033,sig:11,src:000169,op:flip1,pos:73", flags=0x1, fapl=0xb00000000000013, driver=,
drivername=0x0, drivername_size=0x0)
 [#8] 0x5555555564217 → main(argc=, argv=0x7fffffffdfe8)
──────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────────
 0x00005555555f425c in H5AC_unpin_entry (thing=0x55555638fc40) at /hdf5/src/H5AC.c:1419
 1419         if(cache_ptr->log_info->logging)

gef➤  ptype cache_ptr
 type = struct H5C_t {
     uint32_t magic;
     hbool_t flush_in_progress;
     H5C_log_info_t *log_info;
     void *aux_ptr;
     int32_t max_type_id;
     const H5C_class_t * const *class_table_ptr;
     size_t max_cache_size;
     size_t min_clean_size;
     H5C_write_permitted_func_t check_write_permitted;
     hbool_t write_permitted;
     H5C_log_flush_func_t log_flush;
     hbool_t evictions_enabled;
     hbool_t close_warning_received;
     uint32_t index_len;
     size_t index_size;
     uint32_t index_ring_len[6];
     size_t index_ring_size[6];
     size_t clean_index_size;
     size_t clean_index_ring_size[6];
     size_t dirty_index_size;
     size_t dirty_index_ring_size[6];
     H5C_cache_entry_t *index[65536];
     uint32_t il_len;
     size_t il_size;
     H5C_cache_entry_t *il_head;
     H5C_cache_entry_t *il_tail;
     int64_t entries_removed_counter;
     H5C_cache_entry_t *last_entry_removed_ptr;
     H5C_cache_entry_t *entry_watched_for_removal;
     hbool_t slist_changed;
     uint32_t slist_len;
     size_t slist_size;
     uint32_t slist_ring_len[6];
     size_t slist_ring_size[6];
     H5SL_t *slist_ptr;
     uint32_t num_last_entries;
     H5SL_t *tag_list;
     hbool_t ignore_tags;
     uint32_t num_objs_corked;
     uint32_t pl_len;
     size_t pl_size;
     H5C_cache_entry_t *pl_head_ptr;
     H5C_cache_entry_t *pl_tail_ptr;
     uint32_t pel_len;
     size_t pel_size;
     H5C_cache_entry_t *pel_head_ptr;
     H5C_cache_entry_t *pel_tail_ptr;
     uint32_t LRU_list_len;
     size_t LRU_list_size;
     H5C_cache_entry_t *LRU_head_ptr;
     H5C_cache_entry_t *LRU_tail_ptr;
     hbool_t size_increase_possible;
     hbool_t flash_size_increase_possible;
     size_t flash_size_increase_threshold;
```

```
    hbool_t resize_enabled;
    hbool_t cache_full;
    hbool_t size_decreased;
    hbool_t resize_in_progress;
    hbool_t msic_in_progress;
    H5C_auto_size_ctl_t resize_ctl;
    int32_t epoch_markers_active;
    hbool_t epoch_marker_active[10];
    int32_t epoch_marker_ringbuf[11];
    int32_t epoch_marker_ringbuf_first;
    int32_t epoch_marker_ringbuf_last;
    int32_t epoch_marker_ringbuf_size;
    H5C_cache_entry_t epoch_markers[10];
    int64_t cache_hits;
    int64_t cache_accesses;
    H5C_cache_image_ctl_t image_ctl;
    hbool_t serialization_in_progress;
    hbool_t load_image;
    hbool_t image_loaded;
    hbool_t delete_image;
    haddr_t image_addr;
    hsize_t image_len;
    hsize_t image_data_len;
    int64_t entries_loaded_counter;
    int64_t entries_inserted_counter;
    int64_t entries_relocated_counter;
    int64_t entry_fd_height_change_counter;
    uint32_t num_entries_in_image;
    H5C_image_entry_t *image_entries;
    void *image_buffer;
    hbool_t rdfsm_settled;
    hbool_t mdfsm_settled;
    char prefix[32];
} *
gef➤  p cache_ptr->log_info->logging
Cannot access memory at address 0x8
gef➤  p cache_ptr
$1 = (H5C_t *) 0x0
gef➤  i r
rax            0x0  0x0
rbx            0x0  0x0
rcx            0xd0000000000003c  0xd0000000000003c
rdx            0x55555634b010       0x55555634b010
rsi            0x55555626b2ea         0x55555626b2ea
rdi            0x0  0x0
rbp            0x55555638fc40       0x55555638fc40
rsp            0x7fffffffdbd0          0x7fffffffdbd0
r8             0x55555634a138       0x55555634a138
r9             0x72746e65206e6970 0x72746e65206e6970
r10            0x55555634b010       0x55555634b010
r11            0x0  0x0
r12            0xffffffff     0xffffffff
r13            0x0  0x0
r14            0x55555638ea10       0x55555638ea10
r15            0x55555638e8e0       0x55555638e8e0
rip            0x5555555f425c       0x5555555f425c
eflags         0x10206       [ PF IF RF ]
cs             0x33 0x33
ss             0x2b  0x2b
ds             0x0  0x0
es             0x0  0x0
fs             0x0  0x0
gs             0x0  0x0
gef➤  bt
#0  0x000055555555f425c in H5AC_unpin_entry (thing=0x55555638fc40) at /hdf5/src/H5AC.c:1419
#1  0x0000555555577601f1 in H5F__dest (f=f@entry=0x55555638e8e0, flush=flush@entry=0x0) at /hdf5/src/H5Fint.c:1306
#2  0x000055555576ba43 in H5F_open (name=, flags=, fcpl_id=, fapl_id=) at /hdf5/src/H5Fint.c:1824
#3  0x000055555601a78b in H5VL__native_file_open (name=, flags=, fapl_id=, dxpl_id=, req=) at
/hdf5/src/H5VLnative_file.c:99
#4  0x0000555555fdb1b9 in H5VL__file_open (cls=, req=0x0, dxpl_id=0xb0000000000008, fapl_id=0xb0000000000014,
flags=0x1, name=0x55555638d2d0 "POC") at /hdf5/src/H5VLcallback.c:3465
#5  H5VL_file_open (connector_prop=connector_prop@entry=0x7fffffffdd40, name=name@entry=0x55555638d2d0 "POC",
flags=flags@entry=0x1, fapl_id=0xb0000000000014, dxpl_id=0xb0000000000008, req=req@entry=0x0) at
/hdf5/src/H5VLcallback.c:3500
#6  0x0000555555745908 in H5Fopen (filename=filename@entry=0x55555638d2d0 "POC", flags=flags@entry=0x1, fapl_id=,
fapl_id@entry=0xb0000000000014) at /hdf5/src/H5F.c:792
#7  0x00005555555683d8 in h5tools_fopen (fname=0x55555638d2d0 "POC", flags=0x1, fapl=0xb0000000000013, driver=,
drivername=0x0, drivername_size=0x0) at /hdf5/tools/lib/h5tools.c:580
#8  0x0000555555564217 in main (argc=, argv=0x7fffffffdfe8) at /hdf5/tools/src/misc/h5clear.c:342
```

Valgrind Output:

```
==21963== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==21963== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright info
==21963== Command: ./h5clear -s -m POC
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C90: ???
==21963==  Address 0x58c0c90 is 0 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C91: ???
==21963==  Address 0x58c0c91 is 1 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C92: ???
==21963==  Address 0x58c0c92 is 2 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C93: ???
==21963==  Address 0x58c0c93 is 3 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C94: ???
==21963==  Address 0x58c0c94 is 4 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C95: ???
==21963==  Address 0x58c0c95 is 5 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C96: ???
==21963==  Address 0x58c0c96 is 6 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C97: ???
==21963==  Address 0x58c0c97 is 7 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C98: ???
==21963==  Address 0x58c0c98 is 8 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C99: ???
==21963==  Address 0x58c0c99 is 9 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C9A: ???
==21963==  Address 0x58c0c9a is 10 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
```

```
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C9B: ???
==21963==  Address 0x58c0c9b is 11 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C9C: ???
==21963==  Address 0x58c0c9c is 12 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C9D: ???
==21963==  Address 0x58c0c9d is 13 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C9E: ???
==21963==  Address 0x58c0c9e is 14 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0C9F: ???
==21963==  Address 0x58c0c9f is 15 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0CA0: ???
==21963==  Address 0x58c0ca0 is 16 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0CA1: ???
==21963==  Address 0x58c0ca1 is 17 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0CA2: ???
==21963==  Address 0x58c0ca2 is 18 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0CA3: ???
==21963==  Address 0x58c0ca3 is 19 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0CA4: ???
==21963==  Address 0x58c0ca4 is 20 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0CA5: ???
==21963==  Address 0x58c0ca5 is 21 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0A8F: ???
```

```
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0CA6: ???
==21963==  Address 0x58c0ca6 is 22 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0ABF: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0CA7: ???
==21963==  Address 0x58c0ca7 is 23 bytes after a block of size 64 alloc'd
==21963==    at 0x4C2FB0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-amd64-linux.so)
==21963==    by 0x38382F: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x58C0ABF: ???
==21963==    by 0x58C089F: ???
==21963==    by 0x37: ???
==21963==    by 0x4CB5B2: ??? (in /hdf5/build/bin/h5clear)
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0CA8: ???
==21963==  Address 0x58c0ca8 is 24 bytes after a block of size 64 in arena "client"
==21963==
==21963== Invalid read of size 1
==21963==    at 0x318FB7: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x504A81: ??? (in /hdf5/build/bin/h5clear)
==21963==    by 0x16: ???
==21963==    by 0x58C0CA9: ???
==21963==  Address 0x58c0ca9 is 25 bytes after a block of size 64 in arena "client"
==21963==
==21963== Invalid read of size 8
==21963==    at 0x1A825C: ??? (in /hdf5/build/bin/h5clear)
==21963==  Address 0x8 is not stack'd, malloc'd or (recently) free'd
==21963==
==21963==
==21963== Process terminating with default action of signal 11 (SIGSEGV)
==21963==  Access not within mapped region at address 0x8
==21963==    at 0x1A825C: ??? (in /hdf5/build/bin/h5clear)
==21963==  If you believe this happened as a result of a stack
==21963==  overflow in your program's main thread (unlikely but
==21963==  possible), you can try to increase the size of the
==21963==  main thread stack using the --main-stacksize= flag.
==21963==  The main thread stack size used in this run was 8388608.
Segmentation fault
```

Proof of Concept

`./h5clear -s -m $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.