CVE-2020-10809: Heap overflow in decompress.c – HDF5 – 1.13.0

Heap overflow in decompress.c – HDF5 – 1.13.0

Loginsoft-2020-1002

11 March, 2020

CVE Number

CVE-2020-10809

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 `Decompress()` located in `decompress.c`. The same be triggered by sending a crafted file to the gif2h5 binary. It allows an attacker to cause Denial of Service.

SYNOPSIS

We observed that in function Gif2Mem() in the line gifImageDesc[ImageCount-1]->Image = Decompress(gifImageDesc[ImageCount-1], gifHead); from this it calls another function Decompress () located in decompress.c to convert gif to hdf image, here in line OutCode[OutCount++] = Suffix[CurCode]; at the time of assignment operation left side interger pointer OutCode size is much small then right side interger pointer Suffix.

vulnerable Source code

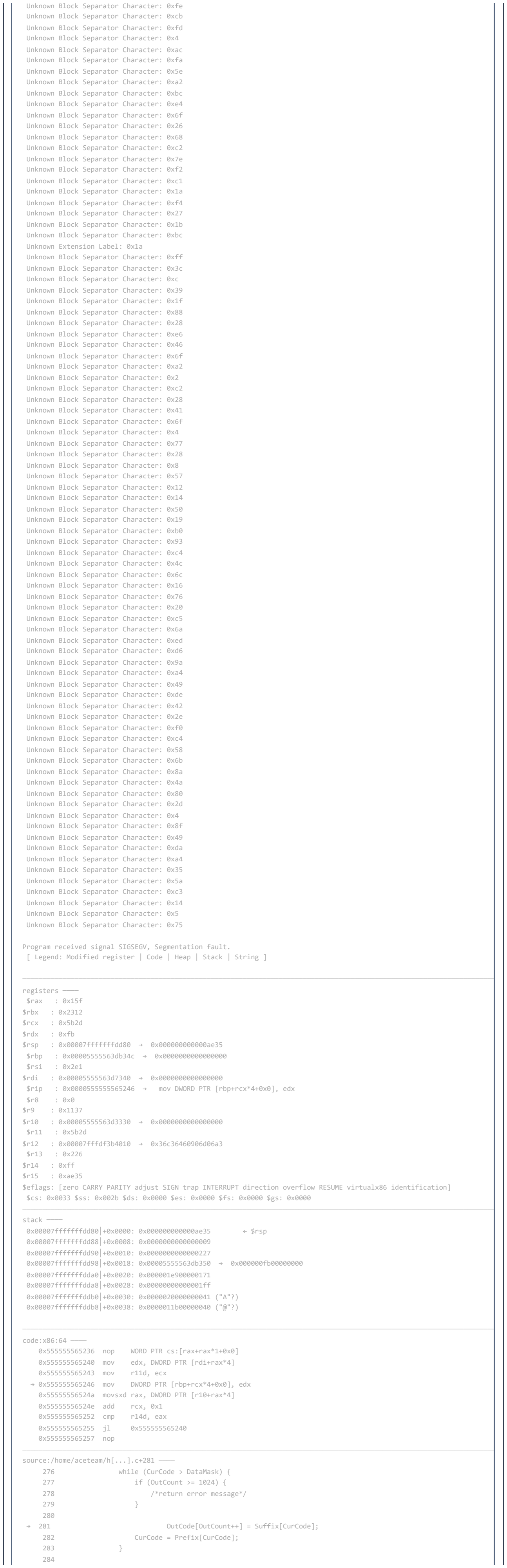
```
      276                   while (CurCode > DataMask) {
     277                   if (OutCount >= 1024) {
     278                       /*return error message*/
     279                   }
     280
 →  281                            OutCode[OutCount++] = Suffix[CurCode];
     282                   CurCode = Prefix[CurCode];
     283               }
     284
    285               /* The last code in the chain is treated as raw data. */
     286               FinChar = CurCode & DataMask;
```

Analysis

DEBUG:

GDB:

```
Starting program: /hdf5/build1/bin/gif2h5 $POC /dev/null
 Unknown Block Separator Character: 0xa
 Unknown Block Separator Character: 0x42
 Unknown Block Separator Character: 0xa0
 Unknown Block Separator Character: 0x8
 Unknown Block Separator Character: 0xf8
 Unknown Block Separator Character: 0x60
 Unknown Block Separator Character: 0xd
 Unknown Block Separator Character: 0xf8
 Unknown Block Separator Character: 0xa0
 Unknown Block Separator Character: 0x8
 Unknown Block Separator Character: 0x2e
 Unknown Block Separator Character: 0x15
 Unknown Block Separator Character: 0xe3
 Unknown Block Separator Character: 0xc
 Unknown Block Separator Character: 0xca
 Unknown Block Separator Character: 0x2
 Unknown Block Separator Character: 0x16
 Unknown Block Separator Character: 0xce
 Unknown Block Separator Character: 0xe3
 Unknown Block Separator Character: 0x34
 Unknown Block Separator Character: 0xee
 Unknown Block Separator Character: 0xa0
 Unknown Block Separator Character: 0xa0
 Unknown Block Separator Character: 0xa5
 Unknown Block Separator Character: 0x50
 Unknown Block Separator Character: 0x64
 Unknown Block Separator Character: 0x60
 Unknown Block Separator Character: 00
 Unknown Block Separator Character: 0x8
 Unknown Block Separator Character: 0xd2
 Unknown Block Separator Character: 0xe4
 Unknown Block Separator Character: 0xee
 Unknown Block Separator Character: 0x22
 Unknown Block Separator Character: 0x98
 Unknown Block Separator Character: 0x4e
 Unknown Block Separator Character: 0x63
 Unknown Block Separator Character: 0x4d
 Unknown Block Separator Character: 0xc3
 Unknown Block Separator Character: 0x44
 Unknown Extension Label: 0x87
 Unknown Block Separator Character: 0xaa
 Unknown Block Separator Character: 0x32
 Unknown Block Separator Character: 0x5c
 Unknown Block Separator Character: 0xd3
 Unknown Block Separator Character: 0xbe
 Unknown Block Separator Character: 0x9a
 Unknown Block Separator Character: 0x75
 Unknown Block Separator Character: 0x3e
 Unknown Block Separator Character: 0xed
 Unknown Block Separator Character: 0x93
 Unknown Block Separator Character: 0xa8
 Unknown Block Separator Character: 0x66
 Unknown Block Separator Character: 0x11
 Unknown Block Separator Character: 0x32
 Unknown Block Separator Character: 0xff
 Unknown Block Separator Character: 0x92
 Unknown Block Separator Character: 0x4a
 Unknown Block Separator Character: 0x98
 Unknown Block Separator Character: 0xfc
 Unknown Block Separator Character: 0xe2
 Unknown Block Separator Character: 0x60
 Unknown Block Separator Character: 0xec
 Unknown Block Separator Character: 0x42
 Unknown Block Separator Character: 0x36
 Unknown Block Separator Character: 0x34
 Unknown Block Separator Character: 0x72
 Unknown Block Separator Character: 0x2d
 Unknown Block Separator Character: 0x62
 Unknown Block Separator Character: 0xe1
 Unknown Block Separator Character: 0x9c
 Unknown Block Separator Character: 0x76
 Unknown Block Separator Character: 0x60
 Unknown Block Separator Character: 0x16
 Unknown Block Separator Character: 0xa
 Unknown Block Separator Character: 0x40
 Unknown Block Separator Character: 0x11
 Unknown Block Separator Character: 0x2e
 Unknown Block Separator Character: 0x41
 Unknown Block Separator Character: 0x11
 Unknown Block Separator Character: 0x5c
 Unknown Block Separator Character: 0x1
 Unknown Block Separator Character: 0xf
 Unknown Block Separator Character: 0x30
 Unknown Block Separator Character: 0x41
 Unknown Block Separator Character: 0x11
 Unknown Block Separator Character: 0x95
 Unknown Block Separator Character: 0x2e
 Unknown Block Separator Character: 0x29
 Unknown Block Separator Character: 0x9c
 Unknown Block Separator Character: 0x2e
 Unknown Block Separator Character: 0x29
 Unknown Block Separator Character: 0x9c
 Unknown Block Separator Character: 0x63
 Unknown Block Separator Character: 0x9
 Unknown Block Separator Character: 0x67
 Unknown Block Separator Character: 0x81
 Unknown Block Separator Character: 0x16
 Unknown Block Separator Character: 0x7a
 Unknown Block Separator Character: 0x1
 Unknown Block Separator Character: 0x65
 Unknown Block Separator Character: 0x58
 Unknown Block Separator Character: 0x46
 Unknown Block Separator Character: 0x18
 Unknown Block Separator Character: 0xce
 Unknown Block Separator Character: 0x2a
 Unknown Block Separator Character: 0xeb
 Unknown Block Separator Character: 0x12
 Unknown Block Separator Character: 0xb
 Unknown Block Separator Character: 0xec
 Unknown Block Separator Character: 0xac
 Unknown Block Separator Character: 0xe6
 Unknown Block Separator Character: 0x41
 Unknown Block Separator Character: 0xe0
 Unknown Block Separator Character: 0xaa
 Unknown Block Separator Character: 0x66
 Unknown Block Separator Character: 0x7c
 Unknown Block Separator Character: 0x92
 Unknown Block Separator Character: 0xae
 Unknown Block Separator Character: 0x82
 Unknown Block Separator Character: 0x12
 Unknown Block Separator Character: 0x60
 Unknown Block Separator Character: 0x3
 Unknown Block Separator Character: 0x89
 Unknown Block Separator Character: 0x28
 Unknown Block Separator Character: 0x17
 Unknown Block Separator Character: 0x64
 Unknown Block Separator Character: 0x28
 Unknown Block Separator Character: 0x97
 Unknown Block Separator Character: 0x86
 Unknown Block Separator Character: 0x25
 Unknown Block Separator Character: 0x90
 Unknown Block Separator Character: 0xf2
 Unknown Block Separator Character: 0x67
 Unknown Block Separator Character: 0x78
 Unknown Block Separator Character: 0x86
 Unknown Block Separator Character: 0x6a
 Unknown Block Separator Character: 0x90
 Unknown Block Separator Character: 0xd2
 Unknown Block Separator Character: 0xee
 Unknown Block Separator Character: 0xc2
 Unknown Block Separator Character: 0xc1
Unknown Block Separator Character: 0xac
Unknown Block Separator Character: 0xc1
Unknown Block Separator Character: 0xb1
Unknown Block Separator Character: 0xc6
Unknown Block Separator Character: 0x6
Unknown Block Separator Character: 0x6d
Unknown Block Separator Character: 0xac
Unknown Block Separator Character: 0x81
Unknown Block Separator Character: 0x17
Unknown Block Separator Character: 0xfa
Unknown Block Separator Character: 0x8e
Unknown Block Separator Character: 0x6c
Unknown Block Separator Character: 0xc6
Unknown Block Separator Character: 0xa6
Unknown Block Separator Character: 0xcd
Unknown Block Separator Character: 00
Unknown Block Separator Character: 0x11
Unknown Block Separator Character: 0x8c
Unknown Block Separator Character: 0x2
Unknown Block Separator Character: 0x7
Unknown Block Separator Character: 0x72
Unknown Block Separator Character: 0x20
Unknown Block Separator Character: 0xcf
Unknown Block Separator Character: 0xf1
Unknown Block Separator Character: 0x32
Unknown Block Separator Character: 0x47
Unknown Block Separator Character: 0x64
Unknown Block Separator Character: 0x94
Unknown Block Separator Character: 0xcb
Unknown Block Separator Character: 00
Unknown Block Separator Character: 0x48
Unknown Block Separator Character: 0x61
Unknown Block Separator Character: 0x2d
Unknown Block Separator Character: 0xa1
Unknown Block Separator Character: 0xab
Unknown Block Separator Character: 0xf3
Unknown Block Separator Character: 0x3a
Unknown Block Separator Character: 0x8f
Unknown Block Separator Character: 0x2e
Unknown Block Separator Character: 0x45
Unknown Block Separator Character: 0xf
Unknown Block Separator Character: 0x32
Unknown Block Separator Character: 0xd
Unknown Block Separator Character: 0x13
Unknown Block Separator Character: 0x2e
Unknown Block Separator Character: 0x83
Unknown Block Separator Character: 0x40
Unknown Block Separator Character: 0x31
Unknown Block Separator Character: 0xf5
Unknown Block Separator Character: 0xd2
Unknown Block Separator Character: 0x2d
Unknown Block Separator Character: 0x61
Unknown Block Separator Character: 0x56
Unknown Block Separator Character: 0x66
Unknown Block Separator Character: 0x49
Unknown Block Separator Character: 0x2f
Unknown Block Separator Character: 0x14
Unknown Block Separator Character: 0xe
Unknown Block Separator Character: 0xf3
Unknown Block Separator Character: 0x1c
Unknown Block Separator Character: 0xa
Unknown Block Separator Character: 0x80
Unknown Block Separator Character: 0x66
Unknown Block Separator Character: 0x4b
Unknown Block Separator Character: 0x2f
Unknown Block Separator Character: 0x14
Unknown Block Separator Character: 0xa
Unknown Block Separator Character: 0x53
Unknown Block Separator Character: 0x2e
Unknown Block Separator Character: 0x9
Unknown Block Separator Character: 0xd3
Unknown Block Separator Character: 0x27
Unknown Block Separator Character: 0x6a
Unknown Block Separator Character: 0x16
Unknown Block Separator Character: 0xf6
Unknown Block Separator Character: 0x80
Unknown Block Separator Character: 0x36
Unknown Block Separator Character: 0x2e
Unknown Block Separator Character: 0x43
Unknown Block Separator Character: 0xa1
Unknown Block Separator Character: 0x66
Unknown Block Separator Character: 0x7b
Unknown Block Separator Character: 0x76
Unknown Block Separator Character: 0xf6
Unknown Block Separator Character: 0xc
Unknown Block Separator Character: 0x53
Unknown Block Separator Character: 0x67
Unknown Block Separator Character: 0x15
Unknown Block Separator Character: 0x53
Unknown Block Separator Character: 0x68
Unknown Block Separator Character: 0xfb
Unknown Block Separator Character: 0xd2
Unknown Block Separator Character: 0x67
Unknown Block Separator Character: 0x6d
Unknown Block Separator Character: 0xd6
Unknown Block Separator Character: 0xdc
Unknown Block Separator Character: 0x64
Unknown Block Separator Character: 0xcf
Unknown Block Separator Character: 0x69
Unknown Block Separator Character: 0x47
Unknown Block Separator Character: 0x4f
Unknown Block Separator Character: 0x30
Unknown Block Separator Character: 0x7d
Unknown Block Separator Character: 0xe7
Unknown Block Separator Character: 0x26
Unknown Block Separator Character: 0xea
Unknown Block Separator Character: 0x81
Unknown Block Separator Character: 0x78
Unknown Block Separator Character: 0xe6
Unknown Block Separator Character: 0x27
Unknown Block Separator Character: 0x1d
Unknown Block Separator Character: 0x3c
Unknown Block Separator Character: 0xf3
Unknown Block Separator Character: 0x7d
Unknown Block Separator Character: 0xf0
Unknown Block Separator Character: 0x88
Unknown Block Separator Character: 0x36
Unknown Block Separator Character: 0x4c
Unknown Block Separator Character: 0x42
Unknown Block Separator Character: 0x34
Unknown Block Separator Character: 0xa5
Unknown Block Separator Character: 0x27
Unknown Block Separator Character: 0xfd
Unknown Block Separator Character: 0x70
Unknown Block Separator Character: 0x13
Unknown Block Separator Character: 0x7b
Unknown Block Separator Character: 0xb4
Unknown Block Separator Character: 0xa7
Unknown Block Separator Character: 0x35
Unknown Block Separator Character: 0x2f
Unknown Block Separator Character: 0xc2
Unknown Block Separator Character: 0x59
Unknown Block Separator Character: 0xcf
Unknown Block Separator Character: 0x56
Unknown Block Separator Character: 0xbe
Unknown Block Separator Character: 0x66
Unknown Block Separator Character: 0x73
Unknown Block Separator Character: 0x7c
Unknown Block Separator Character: 0x14
Unknown Block Separator Character: 0xa2
Unknown Block Separator Character: 0xfb
Unknown Block Separator Character: 0xce
Unknown Block Separator Character: 0xc7
```



```
 Unknown Block Separator Character: 0xfe
 Unknown Block Separator Character: 0xcb
 Unknown Block Separator Character: 0xfd
 Unknown Block Separator Character: 0x4
 Unknown Block Separator Character: 0xac
 Unknown Block Separator Character: 0xfa
 Unknown Block Separator Character: 0x5e
 Unknown Block Separator Character: 0xa2
 Unknown Block Separator Character: 0xbc
 Unknown Block Separator Character: 0xe4
 Unknown Block Separator Character: 0x6f
 Unknown Block Separator Character: 0x26
 Unknown Block Separator Character: 0x68
 Unknown Block Separator Character: 0xc2
 Unknown Block Separator Character: 0x7e
 Unknown Block Separator Character: 0xf2
 Unknown Block Separator Character: 0xc1
 Unknown Block Separator Character: 0x1a
 Unknown Block Separator Character: 0xf4
 Unknown Block Separator Character: 0x27
 Unknown Block Separator Character: 0x1b
 Unknown Block Separator Character: 0xbc
 Unknown Extension Label: 0x1a
 Unknown Block Separator Character: 0xff
 Unknown Block Separator Character: 0x3c
 Unknown Block Separator Character: 0xc
 Unknown Block Separator Character: 0x39
 Unknown Block Separator Character: 0x1f
 Unknown Block Separator Character: 0x88
 Unknown Block Separator Character: 0x28
 Unknown Block Separator Character: 0xe6
 Unknown Block Separator Character: 0x46
 Unknown Block Separator Character: 0x6f
 Unknown Block Separator Character: 0xa2
 Unknown Block Separator Character: 0x2
 Unknown Block Separator Character: 0xc2
 Unknown Block Separator Character: 0x28
 Unknown Block Separator Character: 0x41
 Unknown Block Separator Character: 0x6f
 Unknown Block Separator Character: 0x4
 Unknown Block Separator Character: 0x77
 Unknown Block Separator Character: 0x28
 Unknown Block Separator Character: 0x8
 Unknown Block Separator Character: 0x57
 Unknown Block Separator Character: 0x12
 Unknown Block Separator Character: 0x14
 Unknown Block Separator Character: 0x50
 Unknown Block Separator Character: 0x19
 Unknown Block Separator Character: 0xb0
 Unknown Block Separator Character: 0x93
 Unknown Block Separator Character: 0xc4
 Unknown Block Separator Character: 0x4c
 Unknown Block Separator Character: 0x6c
 Unknown Block Separator Character: 0x16
 Unknown Block Separator Character: 0x76
 Unknown Block Separator Character: 0x20
 Unknown Block Separator Character: 0xc5
 Unknown Block Separator Character: 0x6a
 Unknown Block Separator Character: 0xed
 Unknown Block Separator Character: 0xd6
 Unknown Block Separator Character: 0x9a
 Unknown Block Separator Character: 0xa4
 Unknown Block Separator Character: 0x49
 Unknown Block Separator Character: 0xde
 Unknown Block Separator Character: 0x42
 Unknown Block Separator Character: 0x2e
 Unknown Block Separator Character: 0xf0
 Unknown Block Separator Character: 0xc4
 Unknown Block Separator Character: 0x58
 Unknown Block Separator Character: 0x6b
 Unknown Block Separator Character: 0x8a
 Unknown Block Separator Character: 0x4a
 Unknown Block Separator Character: 0x80
 Unknown Block Separator Character: 0x2d
 Unknown Block Separator Character: 0x4
 Unknown Block Separator Character: 0x8f
 Unknown Block Separator Character: 0x49
 Unknown Block Separator Character: 0xda
 Unknown Block Separator Character: 0xa4
 Unknown Block Separator Character: 0x35
 Unknown Block Separator Character: 0x5a
 Unknown Block Separator Character: 0xc3
 Unknown Block Separator Character: 0x14
 Unknown Block Separator Character: 0x5
 Unknown Block Separator Character: 0x75

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

────────────────────────────────────────────────────────────────────────────────
registers ────
 $rax   : 0x15f
$rbx   : 0x2312
$rcx   : 0x5b2d
$rdx   : 0xfb
$rsp   : 0x00007fffffffdd80  →  0x000000000000ae35
 $rbp   : 0x00005555563db34c  →  0x0000000000000000
 $rsi   : 0x2e1
$rdi   : 0x00005555563d7340  →  0x0000000000000000
 $rip   : 0x0000555555565246  →   mov DWORD PTR [rbp+rcx*4+0x0], edx
 $r8    : 0x0
$r9    : 0x1137
$r10   : 0x00005555563d3330  →  0x0000000000000000
 $r11   : 0x5b2d
$r12   : 0x00007fffdf3b4010  →  0x36c36460906d06a3
 $r13   : 0x226
$r14   : 0xff
$r15   : 0xae35
$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 ────
 0x00007fffffffdd80│+0x0000: 0x000000000000ae35        ← $rsp
 0x00007fffffffdd88│+0x0008: 0x0000000000000009
 0x00007fffffffdd90│+0x0010: 0x0000000000000227
 0x00007fffffffdd98│+0x0018: 0x00005555563db350  →  0x000000fb00000000
 0x00007fffffffdda0│+0x0020: 0x000001e900000171
 0x00007fffffffdda8│+0x0028: 0x00000000000001ff
 0x00007fffffffddb0│+0x0030: 0x0000020000000041 ("A"?)
 0x00007fffffffddb8│+0x0038: 0x0000011b00000040 ("@"?)

────────────────────────────────────────────────────────────────────────────────
code:x86:64 ────
    0x555555565236  nop    WORD PTR cs:[rax+rax*1+0x0]
    0x555555565240  mov    edx, DWORD PTR [rdi+rax*4]
    0x555555565243  mov    r11d, ecx
  → 0x555555565246  mov    DWORD PTR [rbp+rcx*4+0x0], edx
    0x55555556524a  movsxd rax, DWORD PTR [r10+rax*4]
    0x55555556524e  add    rcx, 0x1
    0x555555565252  cmp    r14d, eax
    0x555555565255  jl     0x555555565240
    0x555555565257  nop
────────────────────────────────────────────────────────────────────────────────
source:/home/aceteam/h[...].c+281 ────
     276                while (CurCode > DataMask) {
     277                    if (OutCount >= 1024) {
     278                        /*return error message*/
     279                    }
     280
 →  281                            OutCode[OutCount++] = Suffix[CurCode];
     282                    CurCode = Prefix[CurCode];
     283                }
     284
     286               FinChar = CurCode & DataMask;

────────────────────────────────────────────────────────────────────────────────
threads ────
 [#0] Id 1, Name: "gif2h5", stopped, reason: SIGSEGV

────────────────────────────────────────────────────────────────────────────────
trace ────
 [#0] 0x555555565246 → Decompress(GifImageDesc=0x5555563d2fe0, GifHead=0x5555563d2510)
 [#1] 0x555555567d3a → Gif2Mem(MemGif=, GifMemoryStruct=0x7fffffffdea0)
 [#2] 0x5555555635fb → main(argv=, argc=)

────────────────────────────────────────────────────────────────────────────────
 0x0000555555565246 in Decompress (GifImageDesc=GifImageDesc@entry=0x5555563d2fe0,
GifHead=GifHead@entry=0x5555563d2510) at /hdf5/hl/tools/gif2h5/decompress.c:281
 281                      OutCode[OutCount++] = Suffix[CurCode];

gef➤  bt
 #0  0x0000555555565246 in Decompress (GifImageDesc=GifImageDesc@entry=0x5555563d2fe0,
GifHead=GifHead@entry=0x5555563d2510) at /hdf5/hl/tools/gif2h5/decompress.c:281
 #1  0x0000555555567d3a in Gif2Mem (MemGif=, GifMemoryStruct=0x7fffffffdea0) at
/hdf5/hl/tools/gif2h5/gif2mem.c:184
 #2  0x00005555555635fb in main (argv=, argc=) at /hdf5/hl/tools/gif2h5/gif2hdf.c:100
 gef➤  i r
 rax            0x15f           0x15f
 rbx            0x2312         0x2312
 rcx            0x5b2d         0x5b2d
 rdx            0xfb 0xfb
 rsi            0x2e1            0x2e1
 rdi            0x5555563d7340        0x5555563d7340
 rbp            0x5555563db34c       0x5555563db34c
 rsp            0x7fffffffdd80           0x7fffffffdd80
 r8             0x0   0x0
 r9             0x1137          0x1137
 r10            0x5555563d3330       0x5555563d3330
 r11            0x5b2d         0x5b2d
 r12            0x7fffdf3b4010         0x7fffdf3b4010
 r13            0x226           0x226
 r14            0xff 0xff
 r15            0xae35         0xae35
 rip            0x555555565246        0x555555565246
 eflags         0x10287       [ CF PF SF IF RF ]
 cs             0x33 0x33
 ss             0x2b  0x2b
 ds             0x0   0x0
 es             0x0   0x0
 fs             0x0   0x0
 gs             0x0   0x0
gef➤  x/d OutCode
 0x5555563db350:           0
```

ASAN Output:

```
Unknown Block Separator Character: 0x42
Unknown Block Separator Character: 0xa0
Unknown Block Separator Character: 0x8
Unknown Block Separator Character: 0xf8
Unknown Block Separator Character: 0x60
Unknown Block Separator Character: 0xd
Unknown Block Separator Character: 0xf8
Unknown Block Separator Character: 0xa0
Unknown Block Separator Character: 0x8
Unknown Block Separator Character: 0x2e
Unknown Block Separator Character: 0x15
Unknown Block Separator Character: 0xe3
Unknown Block Separator Character: 0xc
Unknown Block Separator Character: 0xca
Unknown Block Separator Character: 0x2
Unknown Block Separator Character: 0x16
Unknown Block Separator Character: 0xce
Unknown Block Separator Character: 0xe3
Unknown Block Separator Character: 0x34
Unknown Block Separator Character: 0xee
Unknown Block Separator Character: 0xa0
Unknown Block Separator Character: 0xa0
Unknown Block Separator Character: 0xa5
Unknown Block Separator Character: 0x50
Unknown Block Separator Character: 0x64
Unknown Block Separator Character: 0x60
Unknown Block Separator Character: 00
Unknown Block Separator Character: 0x8
Unknown Block Separator Character: 0xd2
Unknown Block Separator Character: 0xe4
Unknown Block Separator Character: 0xee
Unknown Block Separator Character: 0x22
Unknown Block Separator Character: 0x98
Unknown Block Separator Character: 0x4e
Unknown Block Separator Character: 0x63
Unknown Block Separator Character: 0x4d
Unknown Block Separator Character: 0xc3
Unknown Block Separator Character: 0x44
Unknown Extension Label: 0x87
Unknown Block Separator Character: 0xaa
Unknown Block Separator Character: 0x32
Unknown Block Separator Character: 0x5c
Unknown Block Separator Character: 0xd3
Unknown Block Separator Character: 0xbe
Unknown Block Separator Character: 0x9a
Unknown Block Separator Character: 0x75
Unknown Block Separator Character: 0x3e
Unknown Block Separator Character: 0xed
Unknown Block Separator Character: 0x93
Unknown Block Separator Character: 0xa8
Unknown Block Separator Character: 0x66
Unknown Block Separator Character: 0x11
Unknown Block Separator Character: 0x32
Unknown Block Separator Character: 0xff
Unknown Block Separator Character: 0x92
Unknown Block Separator Character: 0x4a
Unknown Block Separator Character: 0x98
Unknown Block Separator Character: 0xfc
Unknown Block Separator Character: 0xe2
Unknown Block Separator Character: 0x60
Unknown Block Separator Character: 0xec
Unknown Block Separator Character: 0x42
Unknown Block Separator Character: 0x36
Unknown Block Separator Character: 0x34
Unknown Block Separator Character: 0x72
Unknown Block Separator Character: 0x2d
Unknown Block Separator Character: 0x62
Unknown Block Separator Character: 0xe1
Unknown Block Separator Character: 0x9c
Unknown Block Separator Character: 0x76
Unknown Block Separator Character: 0x60
Unknown Block Separator Character: 0x16
Unknown Block Separator Character: 0xa
Unknown Block Separator Character: 0x40
Unknown Block Separator Character: 0x11
Unknown Block Separator Character: 0x2e
Unknown Block Separator Character: 0x41
Unknown Block Separator Character: 0x11
Unknown Block Separator Character: 0x5c
Unknown Block Separator Character: 0x1
Unknown Block Separator Character: 0xf
Unknown Block Separator Character: 0x30
Unknown Block Separator Character: 0x41
Unknown Block Separator Character: 0x11
Unknown Block Separator Character: 0x95
Unknown Block Separator Character: 0x2e
Unknown Block Separator Character: 0x29
Unknown Block Separator Character: 0x9c
Unknown Block Separator Character: 0x2e
Unknown Block Separator Character: 0x29
Unknown Block Separator Character: 0x9c
Unknown Block Separator Character: 0x63
Unknown Block Separator Character: 0x9
Unknown Block Separator Character: 0x67
Unknown Block Separator Character: 0x81
Unknown Block Separator Character: 0x16
Unknown Block Separator Character: 0x7a
Unknown Block Separator Character: 0x1
Unknown Block Separator Character: 0x65
Unknown Block Separator Character: 0x58
Unknown Block Separator Character: 0x46
Unknown Block Separator Character: 0x18
Unknown Block Separator Character: 0xce
Unknown Block Separator Character: 0x2a
Unknown Block Separator Character: 0xeb
Unknown Block Separator Character: 0x12
Unknown Block Separator Character: 0xb
Unknown Block Separator Character: 0xec
Unknown Block Separator Character: 0xac
Unknown Block Separator Character: 0xe6
Unknown Block Separator Character: 0x41
Unknown Block Separator Character: 0xe0
Unknown Block Separator Character: 0xaa
Unknown Block Separator Character: 0x66
Unknown Block Separator Character: 0x7c
Unknown Block Separator Character: 0x92
Unknown Block Separator Character: 0xae
Unknown Block Separator Character: 0x82
Unknown Block Separator Character: 0x12
Unknown Block Separator Character: 0x60
Unknown Block Separator Character: 0x3
Unknown Block Separator Character: 0x89
Unknown Block Separator Character: 0x28
Unknown Block Separator Character: 0x17
Unknown Block Separator Character: 0x64
Unknown Block Separator Character: 0x28
Unknown Block Separator Character: 0x97
Unknown Block Separator Character: 0x86
Unknown Block Separator Character: 0x25
Unknown Block Separator Character: 0x90
Unknown Block Separator Character: 0xf2
Unknown Block Separator Character: 0x67
Unknown Block Separator Character: 0x78
Unknown Block Separator Character: 0x86
Unknown Block Separator Character: 0x6a
Unknown Block Separator Character: 0x90
Unknown Block Separator Character: 0xd2
Unknown Block Separator Character: 0xee
Unknown Block Separator Character: 0xc2
Unknown Block Separator Character: 0xc1
Unknown Block Separator Character: 0x6b
Unknown Block Separator Character: 0xac
Unknown Block Separator Character: 0xb1
Unknown Block Separator Character: 0xc6
Unknown Block Separator Character: 0x6
Unknown Block Separator Character: 0x6d
Unknown Block Separator Character: 0xac
Unknown Block Separator Character: 0x81
Unknown Block Separator Character: 0x17
Unknown Block Separator Character: 0xfa
Unknown Block Separator Character: 0x8e
Unknown Block Separator Character: 0x6c
Unknown Block Separator Character: 0xc6
Unknown Block Separator Character: 0xa6
Unknown Block Separator Character: 0xcd
Unknown Block Separator Character: 00
Unknown Block Separator Character: 0x11
Unknown Block Separator Character: 0x8c
Unknown Block Separator Character: 0x2
Unknown Block Separator Character: 0x7
Unknown Block Separator Character: 0x72
Unknown Block Separator Character: 0x20
Unknown Block Separator Character: 0xcf
Unknown Block Separator Character: 0xf1
Unknown Block Separator Character: 0x32
Unknown Block Separator Character: 0x47
Unknown Block Separator Character: 0x64
Unknown Block Separator Character: 0x94
Unknown Block Separator Character: 0xcb
Unknown Block Separator Character: 00
Unknown Block Separator Character: 0x48
Unknown Block Separator Character: 0x61
Unknown Block Separator Character: 0x2d
Unknown Block Separator Character: 0xa1
Unknown Block Separator Character: 0xab
Unknown Block Separator Character: 0xf3
Unknown Block Separator Character: 0x3a
Unknown Block Separator Character: 0x8f
Unknown Block Separator Character: 0x2e
Unknown Block Separator Character: 0x45
Unknown Block Separator Character: 0xf
Unknown Block Separator Character: 0x32
Unknown Block Separator Character: 0xd
Unknown Block Separator Character: 0x13
Unknown Block Separator Character: 0x2e
Unknown Block Separator Character: 0x83
Unknown Block Separator Character: 0x40
Unknown Block Separator Character: 0x31
Unknown Block Separator Character: 0xf5
Unknown Block Separator Character: 0xd2
Unknown Block Separator Character: 0x2d
Unknown Block Separator Character: 0x61
Unknown Block Separator Character: 0x56
Unknown Block Separator Character: 0x66
Unknown Block Separator Character: 0x49
Unknown Block Separator Character: 0x2f
Unknown Block Separator Character: 0x14
Unknown Block Separator Character: 0xe
Unknown Block Separator Character: 0xf3
Unknown Block Separator Character: 0x1c
Unknown Block Separator Character: 0xa
Unknown Block Separator Character: 0x80
Unknown Block Separator Character: 0x66
Unknown Block Separator Character: 0x4b
Unknown Block Separator Character: 0x2f
Unknown Block Separator Character: 0x14
Unknown Block Separator Character: 0xa
Unknown Block Separator Character: 0x53
Unknown Block Separator Character: 0x2e
Unknown Block Separator Character: 0x9
Unknown Block Separator Character: 0xd3
Unknown Block Separator Character: 0x27
Unknown Block Separator Character: 0x6a
Unknown Block Separator Character: 0x16
Unknown Block Separator Character: 0xf6
Unknown Block Separator Character: 0x80
Unknown Block Separator Character: 0x36
Unknown Block Separator Character: 0x2e
Unknown Block Separator Character: 0x43
Unknown Block Separator Character: 0xa1
Unknown Block Separator Character: 0x66
Unknown Block Separator Character: 0x7b
Unknown Block Separator Character: 0x76
Unknown Block Separator Character: 0xf6
Unknown Block Separator Character: 0xc
Unknown Block Separator Character: 0x53
Unknown Block Separator Character: 0x67
Unknown Block Separator Character: 0x15
Unknown Block Separator Character: 0x53
Unknown Block Separator Character: 0x68
Unknown Block Separator Character: 0xfb
Unknown Block Separator Character: 0xd2
Unknown Block Separator Character: 0x67
Unknown Block Separator Character: 0x6d
Unknown Block Separator Character: 0xd6
Unknown Block Separator Character: 0xdc
Unknown Block Separator Character: 0x64
Unknown Block Separator Character: 0xcf
Unknown Block Separator Character: 0x69
Unknown Block Separator Character: 0x47
Unknown Block Separator Character: 0x4f
Unknown Block Separator Character: 0x30
Unknown Block Separator Character: 0x7d
Unknown Block Separator Character: 0xe7
Unknown Block Separator Character: 0x26
Unknown Block Separator Character: 0xea
Unknown Block Separator Character: 0x81
Unknown Block Separator Character: 0x78
Unknown Block Separator Character: 0xe6
Unknown Block Separator Character: 0x27
Unknown Block Separator Character: 0x1d
Unknown Block Separator Character: 0x3c
Unknown Block Separator Character: 0xf3
Unknown Block Separator Character: 0x7d
Unknown Block Separator Character: 0xf0
Unknown Block Separator Character: 0x88
Unknown Block Separator Character: 0x36
Unknown Block Separator Character: 0x4c
Unknown Block Separator Character: 0x42
Unknown Block Separator Character: 0x34
Unknown Block Separator Character: 0xa5
Unknown Block Separator Character: 0x27
Unknown Block Separator Character: 0xfd
Unknown Block Separator Character: 0x70
Unknown Block Separator Character: 0x13
Unknown Block Separator Character: 0x7b
Unknown Block Separator Character: 0xb4
Unknown Block Separator Character: 0xa7
Unknown Block Separator Character: 0x35
Unknown Block Separator Character: 0x2f
Unknown Block Separator Character: 0xc2
Unknown Block Separator Character: 0x59
Unknown Block Separator Character: 0xcf
Unknown Block Separator Character: 0x56
Unknown Block Separator Character: 0xbe
Unknown Block Separator Character: 0x66
Unknown Block Separator Character: 0x73
Unknown Block Separator Character: 0x7c
Unknown Block Separator Character: 0x14
Unknown Block Separator Character: 0xa2
Unknown Block Separator Character: 0xfb
Unknown Block Separator Character: 0xce
Unknown Block Separator Character: 0xc7
Unknown Block Separator Character: 0xd1
Unknown Block Separator Character: 0xfe
```

```
 Unknown Block Separator Character: 0xfd
 Unknown Block Separator Character: 0x4
 Unknown Block Separator Character: 0xac
 Unknown Block Separator Character: 0xfa
 Unknown Block Separator Character: 0x5e
 Unknown Block Separator Character: 0xa2
 Unknown Block Separator Character: 0xbc
 Unknown Block Separator Character: 0xe4
 Unknown Block Separator Character: 0x6f
 Unknown Block Separator Character: 0x26
 Unknown Block Separator Character: 0x68
 Unknown Block Separator Character: 0xc2
 Unknown Block Separator Character: 0x7e
 Unknown Block Separator Character: 0xf2
 Unknown Block Separator Character: 0xc1
 Unknown Block Separator Character: 0x1a
 Unknown Block Separator Character: 0xf4
 Unknown Block Separator Character: 0x27
 Unknown Block Separator Character: 0x1b
 Unknown Block Separator Character: 0xbc
 Unknown Extension Label: 0x1a
 Unknown Block Separator Character: 0xff
 Unknown Block Separator Character: 0x3c
 Unknown Block Separator Character: 0xc
 Unknown Block Separator Character: 0x39
 Unknown Block Separator Character: 0x1f
 Unknown Block Separator Character: 0x88
 Unknown Block Separator Character: 0x28
 Unknown Block Separator Character: 0xe6
 Unknown Block Separator Character: 0x46
 Unknown Block Separator Character: 0x6f
 Unknown Block Separator Character: 0xa2
 Unknown Block Separator Character: 0x2
 Unknown Block Separator Character: 0xc2
 Unknown Block Separator Character: 0x28
 Unknown Block Separator Character: 0x41
 Unknown Block Separator Character: 0x6f
 Unknown Block Separator Character: 0x4
 Unknown Block Separator Character: 0x77
 Unknown Block Separator Character: 0x28
 Unknown Block Separator Character: 0x8
 Unknown Block Separator Character: 0x57
 Unknown Block Separator Character: 0x12
 Unknown Block Separator Character: 0x14
 Unknown Block Separator Character: 0x50
 Unknown Block Separator Character: 0x19
 Unknown Block Separator Character: 0xb0
 Unknown Block Separator Character: 0x93
 Unknown Block Separator Character: 0xc4
 Unknown Block Separator Character: 0x4c
 Unknown Block Separator Character: 0x6c
 Unknown Block Separator Character: 0x16
 Unknown Block Separator Character: 0x76
 Unknown Block Separator Character: 0x20
 Unknown Block Separator Character: 0xc5
 Unknown Block Separator Character: 0x6a
 Unknown Block Separator Character: 0xed
 Unknown Block Separator Character: 0xd6
 Unknown Block Separator Character: 0x9a
 Unknown Block Separator Character: 0xa4
 Unknown Block Separator Character: 0x49
 Unknown Block Separator Character: 0xde
 Unknown Block Separator Character: 0x42
 Unknown Block Separator Character: 0x2e
 Unknown Block Separator Character: 0xf0
 Unknown Block Separator Character: 0xc4
 Unknown Block Separator Character: 0x58
 Unknown Block Separator Character: 0x6b
 Unknown Block Separator Character: 0x8a
 Unknown Block Separator Character: 0x4a
 Unknown Block Separator Character: 0x80
 Unknown Block Separator Character: 0x2d
 Unknown Block Separator Character: 0x4
 Unknown Block Separator Character: 0x8f
 Unknown Block Separator Character: 0x49
 Unknown Block Separator Character: 0xda
 Unknown Block Separator Character: 0xa4
 Unknown Block Separator Character: 0x35
 Unknown Block Separator Character: 0x5a
 Unknown Block Separator Character: 0xc3
 Unknown Block Separator Character: 0x14
 Unknown Block Separator Character: 0x5
 Unknown Block Separator Character: 0x75
 =================================================================
 ==519==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x621000003900 at pc 0x55d0424f140b bp
0x7ffc1c603e10 sp 0x7ffc1c603e00
 WRITE of size 4 at 0x621000003900 thread T0
     #0 0x55d0424f140a in Decompress /hdf5/hl/tools/gif2h5/decompress.c:281
     #1 0x55d0424f163d in Gif2Mem /hdf5/hl/tools/gif2h5/gif2mem.c:184
     #2 0x55d0424ed039 in main /hdf5/hl/tools/gif2h5/gif2hdf.c:100
     #3 0x7f8edf4f6b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
     #4 0x55d0424f0ac9 in _start (/hdf5/build/bin/gif2h5+0x156ac9)

0x621000003900 is located 0 bytes to the right of 4096-byte region [0x621000002900,0x621000003900)
 allocated by thread T0 here:
     #0 0x7f8edff46d38 in __interceptor_calloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xded38)
     #1 0x55d0424f0e60 in Decompress /hdf5/hl/tools/gif2h5/decompress.c:170

SUMMARY: AddressSanitizer: heap-buffer-overflow /hdf5/hl/tools/gif2h5/decompress.c:281 in Decompress
 Shadow bytes around the buggy address:
   0x0c427fff86d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   0x0c427fff86e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   0x0c427fff86f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   0x0c427fff8700: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   0x0c427fff8710: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 =>0x0c427fff8720:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c427fff8730: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c427fff8740: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c427fff8750: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c427fff8760: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
   0x0c427fff8770: 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
 ==519==ABORTING
```

Proof of Concept

`./gif2h5 $POC /dev/null`

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