Talos Vulnerability Report

TALOS-2021-1295

Disc Soft Ltd Daemon Tools Pro ISO Parsing memory corruption vulnerability

AUGUST 17, 2021

CVE NUMBER

CVE-2021-21832

Summary

A memory corruption vulnerability exists in the ISO Parsing functionality of Disc Soft Ltd Deamon Tools Pro 8.3.0.0767. A specially crafted malformed file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability.

Tested Versions

Disc Soft Ltd Daemon Tools Pro 8.3.0.0767

Product URLs

https://www.daemon-tools.cc

CVSSv3 Score

8.1 - CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CWE

CWE-680 - Integer Overflow to Buffer Overflow

Details

DAEMON Tools Pro is a powerful and professional emulation software to work with disc images and virtual drives. It allows mounting of ISO images on Windows systems.

When parsing a specifically crafted ISO file it is possible to cause a memory corruption. This is due to an integer overflow during a malloc operation:

```
.text:00000000000A25D7                 mov     ecx, [rbp+880h+var_8F6]                ; taken from the ISO Directory record (size)
.text:00000000000A25DA                 shl     ecx, 4            ; unsigned __int64   ; integer overflow (32bit reg)
.text:00000000000A25DD                 call    j_??2@YAPEAX_K@Z ; operator new(unsigned __int64)
.text:00000000000A25E2                 mov     rdi, rax                               ; possible to allocate with size=0
```

Initial ECX value is taken directly from the ISO file - ISO Directory record (size). Due to SHL operation and 32-bit register size it is possible to cause an integer overflow and for example allocate a memory region with size=0.
This leads to heap memory corruption when the allocated buffer is written to, here:

```
.text:000000000009A9B2 loc_9A9B2:                              ; CODE XREF: bad_function+300↑j
.text:000000000009A9B2                 movsxd  rdx, r8d
.text:000000000009A9B5                 mov     eax, r13d
.text:000000000009A9B8                 sub     eax, r8d
.text:000000000009A9BB                 add     rdx, rcx        ; Src
.text:000000000009A9BE                 mov     rcx, [rsp+88h+AllocatedMem] ; Dst
.text:000000000009A9C6                 movsxd  rbx, eax
.text:000000000009A9C9                 mov     r8, rbx         ; Size
.text:000000000009A9CC                 call    memmove         ;
.text:000000000009A9D1                 mov     r9, [rsp+88h+arg_10]
.text:000000000009A9D9                 xor     r8d, r8d
```

And this leads to the following crash:

```
(40e8.3480): Access violation - code c0000005 (!!! second chance !!!)
Engine!FillWaveHeader+0x13207:
00007ffc`8efa25b7 f3a4            rep movs byte ptr [rdi],byte ptr [rsi]
0:000> r
rax=000002662b5e7be0 rbx=0000000000000800 rcx=00000000000003e0
rdx=0000000000d31350 rsi=000002662c319350 rdi=000002662b5e8000
rip=00007ffc8efa25b7 rsp=000000df0e2fcad8 rbp=000002662c318f20
 r8=000002662c4f0c80  r9=0000000000007000 r10=000002662c318f30
r11=0000000000000001 r12=0000000000000000 r13=0000000000000800
r14=000002662c317c00 r15=0000000000000005
iopl=0         nv up ei pl nz na pe cy
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010201
Engine!FillWaveHeader+0x13207:
00007ffc`8efa25b7 f3a4            rep movs byte ptr [rdi],byte ptr [rsi]
0:000> db @rdi
00000266`2b5e8000  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????
00000266`2b5e8010  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????
00000266`2b5e8020  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????
00000266`2b5e8030  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????
00000266`2b5e8040  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????
00000266`2b5e8050  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????
00000266`2b5e8060  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????
00000266`2b5e8070  ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??  ????????????????
```

Crash Information

```
    0:000> !analyze -v
    *******************************************************************************
    *                                                                             *
    *                        Exception Analysis                                   *
    *                                                                             *
    *******************************************************************************


    KEY_VALUES_STRING: 1

        Key  : AV.Fault
        Value: Write

        Key  : Analysis.CPU.mSec
        Value: 86952

        Key  : Analysis.DebugAnalysisManager
        Value: Create

        Key  : Analysis.Elapsed.mSec
        Value: 117195

        Key  : Analysis.Init.CPU.mSec
        Value: 7015

        Key  : Analysis.Init.Elapsed.mSec
        Value: 415009

        Key  : Analysis.Memory.CommitPeak.Mb
        Value: 514

        Key  : Timeline.OS.Boot.DeltaSec
        Value: 448861

        Key  : Timeline.Process.Start.DeltaSec
        Value: 423

        Key  : WER.OS.Branch
        Value: vb_release

        Key  : WER.OS.Timestamp
        Value: 2019-12-06T14:06:00Z

        Key  : WER.OS.Version
        Value: 10.0.19041.1

        Key  : WER.Process.Version
        Value: 8.3.0.767


    NTGLOBALFLAG:  0

    PROCESS_BAM_CURRENT_THROTTLED: 0

    PROCESS_BAM_PREVIOUS_THROTTLED: 0

    APPLICATION_VERIFIER_FLAGS:  0

    EXCEPTION_RECORD:  (.exr -1)
    ExceptionAddress: 00007ffc8efa25b7 (Engine!FillWaveHeader+0x0000000000013207)
       ExceptionCode: c0000005 (Access violation)
      ExceptionFlags: 00000000
    NumberParameters: 2
       Parameter[0]: 0000000000000001
       Parameter[1]: 000002662b5e8000
    Attempt to write to address 000002662b5e8000

    FAULTING_THREAD:  00003480

    PROCESS_NAME:  DTPro.exe

    WRITE_ADDRESS:  000002662b5e8000

    ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p. The memory could not be %s.

    EXCEPTION_CODE_STR:  c0000005

    EXCEPTION_PARAMETER1:  0000000000000001

    EXCEPTION_PARAMETER2:  000002662b5e8000

    STACK_TEXT:  
    000000df`0e2fcad8 00007ffc`8eeca9d1     : 000000df`0e2fd9c0 00000000`00000000 00000266`31ac6740 

00000266`31b46e80 : Engine!FillWaveHeader+0x13207
    000000df`0e2fcae0 00007ffc`8eed2634     : 00000000`00000002 00000000`00008000 00000000`00007000 
00000266`2b5e7be0 : Engine+0x8a9d1
    000000df`0e2fcb70 00007ffc`8eece788     : 00000000`ffffffff 000000df`0e2fd600 00000000`ffffffff 
00000266`2c33d80c : Engine+0x92634
    000000df`0e2fd500 00007ffc`8eece848     : 00000000`00000000 00007ffc`8eed0000 00000266`2c4f0801 
00007ffc`e3093433 : Engine+0x8e788
    000000df`0e2fd930 00007ffc`8ee9a0a5     : 000000df`0e2fda00 00000266`2c33c4d0 00000266`31bc92c8 
00000266`2c33c4d0 : Engine+0x8e848
    000000df`0e2fd9c0 00007ffc`8ee9e187     : 00000266`31b26128 00000000`00000000 00000266`31a99d28 
00000266`2c4f0bd8 : Engine+0x5a0a5
    000000df`0e2fda80 00007ffc`8ee6e2b3     : 00000000`00000000 00000000`00000000 00000266`31bc6940 
000000df`0e2fdb98 : Engine+0x5e187
    000000df`0e2fdab0 00007ff7`a4f45e0e     : 00000266`2b5e6c90 00000266`2b5e6c90 ffffffff`ffffffff 
00000000`00000000 : Engine+0x2e2b3
    000000df`0e2fdb10 00007ff7`a4f473dc     : 000000df`0e2fe270 00007ff7`a5522900 00007ffc`8f014a38 
000000df`0e2fe1a8 : DTPro+0x35e0e
    000000df`0e2fe150 00007ff7`a4f44254     : 00000266`2955f738 00000266`2955f620 00000000`00000000 
00000000`00000000 : DTPro+0x373dc
    000000df`0e2fecd0 00007ff7`a4f4c22b     : 00000266`2955f620 00000000`00000187 00000000`00000000 
00007ff7`a4fecdbd : DTPro+0x34254
    000000df`0e2fed10 00007ff7`a4f58ad6     : 00000266`2955f620 00000000`00000000 00007ff7`a560ffd8 
00007ff7`a4ff0e07 : DTPro+0x3c22b
    000000df`0e2fed50 00007ff7`a4f1a07c     : 00000000`00000000 00000266`2955f530 00000000`00000187 
00000000`00000000 : DTPro+0x48ad6
    000000df`0e2fed90 00007ff7`a4f60492     : 00007ff7`a4f60460 00000000`00000000 00000000`00000187 
00000000`00000000 : DTPro+0xa07c
    000000df`0e2fedd0 00007ff7`a4fc940c     : 00000000`00000000 00000000`00000000 00000000`00000187 
00000266`2c3129e0 : DTPro+0x50492
```

```
    000000df`0e2fee60 00007ff7`a4fe695a     : 00000266`2955f350 00000000`00000187 00000000`00000187
00000000`00000000 : DTPro+0xb940c
    000000df`0e2feef0 00007ff7`a4fca6f7     : 00007ff7`a4fe68cc 000000df`0e2ff020 00000000`00000111
00000000`00000000 : DTPro+0xd695a
    000000df`0e2fef20 00007ff7`a4fccad6     : 00007ff7`a4fca688 00000000`00000000 00000000`00000187
00000266`2955f350 : DTPro+0xba6f7
    000000df`0e2ff0b0 00007ff7`a4fc5da1     : 00000000`00000000 00007ff7`a4fcca88 00000000`00000187
00007ff7`a560ffb0 : DTPro+0xbcad6
    000000df`0e2ff100 00007ff7`a4fc6898     : 00000266`2948a130 00007ff7`a4fd62d8 00000000`04bc07bc
00000000`fffffff0 : DTPro+0xb5da1
    000000df`0e2ff1d0 00007ffc`e31ce858     : 00000000`00000001 00000000`00000187 00000000`00000000
00000000`00000000 : DTPro+0xb6898
    000000df`0e2ff210 00007ffc`e31ce4ee     : ffffffff`fffffffe 00007ff7`a4fc6844 00000000`04bc07bc
000000df`00000111 : USER32!UserCallWinProcCheckWow+0x2f8
    000000df`0e2ff3a0 00007ff7`a51ea323     : 00000266`29577650 00000000`00000000 00000000`00000000
00007ff7`a4fc4cf4 : USER32!CallWindowProcW+0x8e
    000000df`0e2ff3f0 00007ff7`a51eb68a     : 00000266`2c3129e0 00000266`29496a78 000000df`0e2ff4f0
00000266`549fca11 : DTPro+0x2da323
    000000df`0e2ff470 00007ffc`e31ce858     : 00000266`29577650 00000000`00000001 00000000`00000187
00000000`00000000 : DTPro+0x2db68a
    000000df`0e2ff4e0 00007ffc`e31ce299     : 00000266`29496a38 00007ff7`a51eb5f0 00000000`04bc07bc
00007ff7`00000111 : USER32!UserCallWinProcCheckWow+0x2f8
    000000df`0e2ff670 00007ff7`a4fd6732     : 00007ff7`a51eb5f0 00000266`29496a38 00000000`00000000
00007ff7`a561bfb0 : USER32!DispatchMessageWorker+0x249
    000000df`0e2ff6f0 00007ff7`a4fd708f     : 00007ff7`a4fd7004 00000000`00000002 00000000`00000000
0000a52e`ae736e87 : DTPro+0xc6732
    000000df`0e2ff720 00007ff7`a540d88a     : 00007ff7`a4fdd0e4 00007ff7`a4f10000 00000000`00000000
00000266`294823d4 : DTPro+0xc708f
    000000df`0e2ff770 00007ff7`a517b923     : 00000000`00000001 00000000`00000000 00000000`00000000
00000000`00000000 : DTPro+0x4fd88a
    000000df`0e2ff7b0 00007ffc`e4347034     : 00000000`00000000 00000000`00000000 00000000`00000000
00000000`00000000 : DTPro+0x26b923
    000000df`0e2ff7f0 00007ffc`e5082651     : 00000000`00000000 00000000`00000000 00000000`00000000
00000000`00000000 : KERNEL32!BaseThreadInitThunk+0x14
    000000df`0e2ff820 00000000`00000000     : 00000000`00000000 00000000`00000000 00000000`00000000
00000000`00000000 : ntdll!RtlUserThreadStart+0x21


    STACK_COMMAND:  ~0s ; .cxr ; kb

    SYMBOL_NAME:  Engine!FillWaveHeader+13207

    MODULE_NAME: Engine

    IMAGE_NAME:  Engine.dll

    FAILURE_BUCKET_ID:  INVALID_POINTER_WRITE_STRING_DEREFERENCE_c0000005_Engine.dll!FillWaveHeader

    OS_VERSION:  10.0.19041.1

    BUILDLAB_STR:  vb_release

    OSPLATFORM_TYPE:  x64

    OSNAME:  Windows 10

    IMAGE_VERSION:  8.3.0.767

    FAILURE_ID_HASH:  {00d4a20e-1ec2-1efc-2848-4383153988d0}

    Followup:     MachineOwner
    ---------
```

Timeline

2021-05-21 - Vendor Disclosure

2021-07-23 - Vendor Patched

2021-08-17 - Public Release

CREDIT

Discovered by Piotr Bania of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

NEXT REPORT

TALOS-2021-1297

TALOS-2021-1346