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

..	
Full_dbg_info.txt	3 years ago
README.md	3 years ago
zuff.vpk	3 years ago

README.md

CVE-2020-7951

Valve Dota 2 (meshsystem.dll) before 7.23e 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:

```
(319c.1a04): 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+0x224b0:
00007ffa`59c8ef20 0fb70453        movzx   eax,word ptr [rbx+rdx*2] ds:00000151`ab7934e9=????
0:000> r
rax=0000000000000000 rbx=00000151ab7934e9 rcx=0000000000000001
rdx=0000000000000000 rsi=000001513705c270 rdi=0000000000000000
rip=00007ffa59c8ef20 rsp=0000002b5b49d500 rbp=0000000044444444
 r8=0000000000000000  r9=0000000000008000 r10=0000000000000240
r11=0000002b5b49b990 r12=0000000000000000 r13=000001513ed22400
r14=000001513ed22528 r15=0000000041414141
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+0x224b0:
00007ffa`59c8ef20 0fb70453        movzx   eax,word ptr [rbx+rdx*2] ds:00000151`ab7934e9=????
```

Full debug information

Description

In this exception we can control register rbp (rbp=0000000044444444). 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 register r15 it could help for exploitation this vulnerability.

rbp register is overwritten by the value of the zuff.vpk (offset 0x0000ec1e)

r15 register is overwritten by the value of the zuff.vpk (offset 0x0000ec16)

Timeline:

30.04.2019 - Report to hackerone

- ignore
- ignore
- ignore

24.01.2020 - Disclose vulnerability details

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