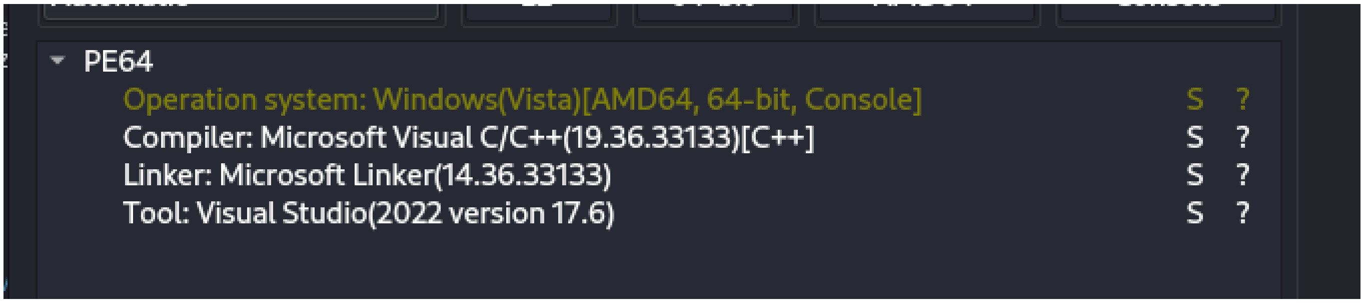
Trex game - idekctf 2024

Challenge Author: Elvis

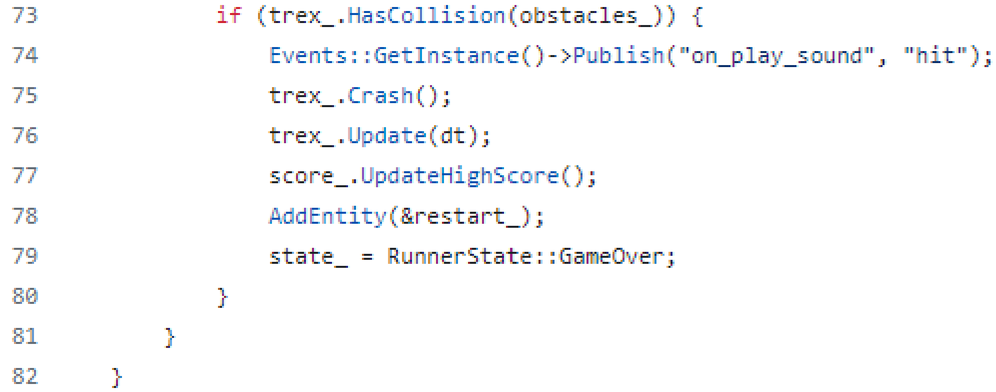
The check collision instruction within the UpdateRunning function in the main_stage class can be manipulated by changing a simple jump instruction in x64dbg. Once the collision event has been patched just let the dinosaur run until the score hits 6969. Once you hit 6969 the file name changes to the flag for the challenge. Changing the score of the dinosaur doesn't exactly work because you must have hit 6969 while running. Finishing the game with a score higher than 6969 does not matter. You must hit the score while the dinosaur is actively running. It takes some waiting but it works.

File info: Detect It Easy



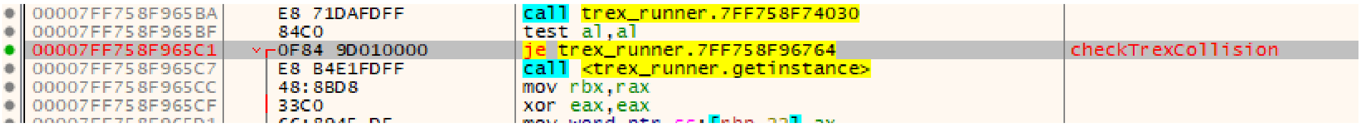
```
PE64
    Operation system: Windows(Vista)[AMD64, 64-bit, Console]    S ?
    Compiler: Microsoft Visual C/C++(19.36.33133)[C++]          S ?
    Linker: Microsoft Linker(14.36.33133)                       S ?
    Tool: Visual Studio(2022 version 17.6)                      S ?
```

Source Code of instruction being patched



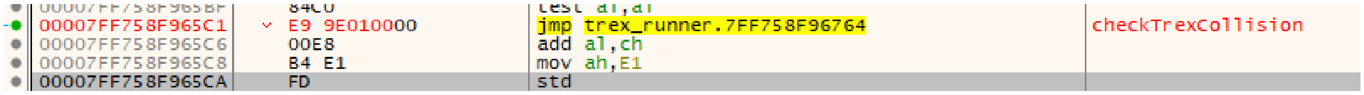
```
            if (trex_.HasCollision(obstacles_)) {
                Events::GetInstance()->Publish("on_play_sound", "hit");
                trex_.Crash();
                trex_.Update(dt);
                score_.UpdateHighScore();
                AddEntity(&restart_);
                state_ = RunnerState::GameOver;
            }
        }
    }
```

JE instruction at 00007FF758F965C1 can be changed to a JMP instruction and collision is removed.



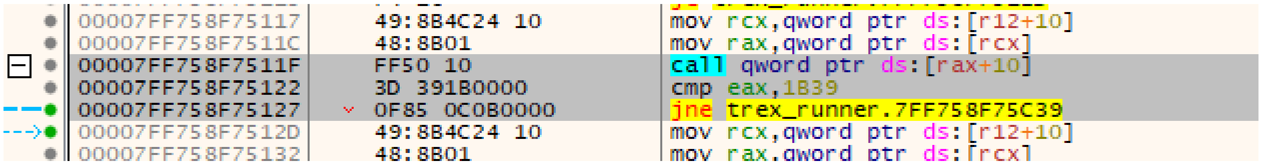
```
00007FF758F965BA   E8 71DAFDFF     call trex_runner.7FF758F74030
00007FF758F965BF   84C0            test al,al
00007FF758F965C1   0F84 9D010000   je trex_runner.7FF758F96764      checkTrexCollision
00007FF758F965C7   E8 B4E1FDFF     call <trex_runner.getinstance>
00007FF758F965CC   48:8BD8         mov rbx,rax
00007FF758F965CF   33C0            xor eax,eax
```

Once the instruction is patched it should look something like this.



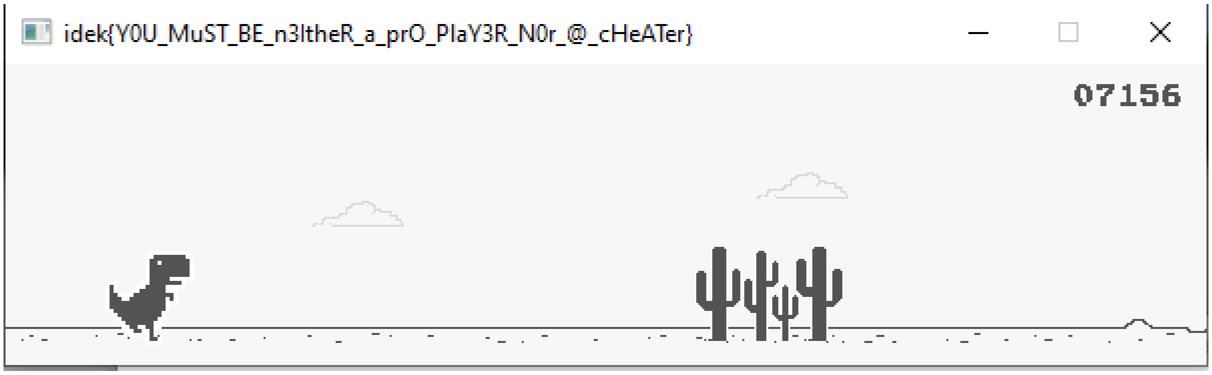
```
00007FF758F965BF   84C0            test al,al
00007FF758F965C1   E9 9E010000     jmp trex_runner.7FF758F96764     checkTrexCollision
00007FF758F965C6   00E8            add al,ch
00007FF758F965C8   B4 E1           mov ah,E1
00007FF758F965CA   FD              std
```

Check that the score is at 6969 starts at 00007FF758F7511F



```
00007FF758F75117    49:8B4C24 10     mov rcx,qword ptr ds:[r12+10]
00007FF758F7511C    48:8B01          mov rax,qword ptr ds:[rcx]
00007FF758F7511F    FF50 10          call qword ptr ds:[rax+10]
00007FF758F75122    3D 391B0000      cmp eax,1B39
00007FF758F75127    0F85 0C0B0000    jne trex_runner.7FF758F75C39
00007FF758F7512D    49:8B4C24 10     mov rcx,qword ptr ds:[r12+10]
00007FF758F75132    48:8B01          mov rax,qword ptr ds:[rcx]
```

Flag outputs to the process title.



idek{Y0U_MuST_BE_n3ItheR_a_prO_PlaY3R_N0r_@_cHeATer}