

simpleVM

发表于 2021-05-25 更新于 2021-05-26 分类于 [Challenge](#) , [2021](#) , [第四届红帽杯网络安全大赛](#) , [Pwn Challenge](#) | [2021](#) | [第四届红帽杯网络安全大赛](#) | [Pwn](#) | [simpleVM](#)

[点击此处](#) 获得更好的阅读体验

WriteUp来源

来自 [Eqgie](#) 的 [博客](#)

题目描述

Hack llvm!

题目考点

- LLVM Pass

解题思路

这里的漏洞出在LLVMPass, LLVM核心库提供了一些"Pass"类让开发者可以去继承然后实现想要的功能。主要的作用就是把编译过程中间的**IR**喂给自定义的Pass从而进行一些针对性的、机器无关的优化。这题的Pass实现了一个由push pop store load add min组成的虚拟机, 由于没有边界限制, 且主程序没开PIE保护, 所以很容易进行任意地址读写。

README.txt

```
1 Hack LLVM!
2
3 Docker Guidance:
4
5 FROM ubuntu:18.04
6
7 RUN sed -i "s/http://archive.ubuntu.com/http://mirrors.tuna.tsinghua.edu.cn/g" /etc/apt/sources.list && \
8     apt-get update && apt-get -y dist-upgrade && \
9     apt-get install -y lib32z1 xinetd libseccomp-dev libseccomp2 seccomp clang-8 opt llvm-8 python
10
11 once your exp.bc(bitcode file) is uploaded
12
13 Sever will execute `opt-8 -load ./VMPass.so -VMPass ./exp.bc`
```

exp.c

```
1 void push(int a);
2 void pop(int a);
3 void store(int a);
4 void load(int a);
5 void add(int a, int b);
6 void min(int a, int b);
7
8 void o0o0o0o0() {
9     add(1, 0x77e100);
10    load(1);
11    add(2, 0x72a9c);
12    store(1);
13 }
```

exp.bc

```
1 ; ModuleID = 'exp.c'
2 source_filename = "exp.c"
3 target datalayout = "e-m:e-i64:64-f80:128-n8:16:32:64-S128"
4 target triple = "x86_64-pc-linux-gnu"
5
6 ; Function Attrs: noinline nounwind optnone uwtable
7 define void @o0o0o0o0() #0 {
8     call void @add(i32 1, i32 7856384)
9     call void @load(i32 1)
10    call void @add(i32 2, i32 469660)
11    call void @store(i32 1)
12    ret void
13 }
14
15 declare void @add(i32, i32) #1
16
17 declare void @load(i32) #1
18
19 declare void @store(i32) #1
20
21 attributes #0 = { noinline nounwind optnone uwtable "correctly-rounded-divide-sqrt-fp-math"="false" "disable-tail-calls"="false" "less-precise-fpmad"="false" "no-frame-po.
22 attributes #1 = { "correctly-rounded-divide-sqrt-fp-math"="false" "disable-tail-calls"="false" "less-precise-fpmad"="false" "no-frame-pointer-elim"="true" "no-frame-pointe
23
24 !llvm.module.flags = !{!0}
25 !llvm.ident = !{!1}
26
27 !0 = !{i32 1, !"wchar_size", i32 4}
28 !1 = !{!"clang version 6.0.0-lubuntu2 (tags/RELEASE_600/final)"}
29
```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge2021/第四届红帽杯网络安全大赛/Pwn/c6bfrsSHD72JgKDAtmMSZS.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

#Challenge #2021 #Pwn #第四届红帽杯网络安全大赛

[默认口令](#)

[ezRev](#)