Security critical software has double-fetch bugs
- OS kernels, hypervisors, TEEs
- High-impact bugs
- CVE-2016-8438 – “Complete compromise”
- CVE-2020-25212 – “… information disclosure”
- Easy to exploit
- Only requires two user threads

```
sigaction(signum, *act, *oldact)
    if(*(act->X) < len){...}
    ...
    access(array[*act->X]);
```

Toy TOCTTOU bug

"Through a syscall's lifetime, every read to a userspace object will return the same value."

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
rd(X) = 0
    X=42
syscall end
```

Target

Attacker

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
rd(X) = 42
    X=42
wr(X, 42)
    X=42
```

Midas Invariant

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
syscall end
```

Target

Attacker

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
rd(X) = 42
    X=42
wr(X, 42)
    X=42
```

Evaluation

- Protects against CVE-2016-2516
- Low 3.4% average overhead on benchmarks

Minimal changes to kernel codebase
- Mostly userspace copy, page fault handler functions
- 17 lines modified, 1100 lines added

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
wr(X, 42)
    X=42
```

Target

Attacker

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
syscall end
```

Page State Machine

Transitions:
1. Syscall read → Snapshot
2. Any write → Copy
3. Syscall end → Snapshot

Snapshooting is common (cheap)
Copying is rare

Minimal changes to kernel codebase
- Mostly userspace copy, page fault handler functions
- 17 lines modified, 1100 lines added

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
syscall end
```

Target

Attacker

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
wr(X, 42)
    X=42
```

Midas Invariant

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
syscall end
```

Target

Attacker

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
syscall end
```

Midas Invariant

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
syscall end
```

Target

Attacker

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
wr(X, 42)
    X=42
```

Midas Invariant

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
syscall end
```

Target

Attacker

```
syscall
    X=0
rd(X) = 0
    X=0
rd(X) = 0
    X=42
wr(X, 42)
    X=42
```

Midas Invariant