

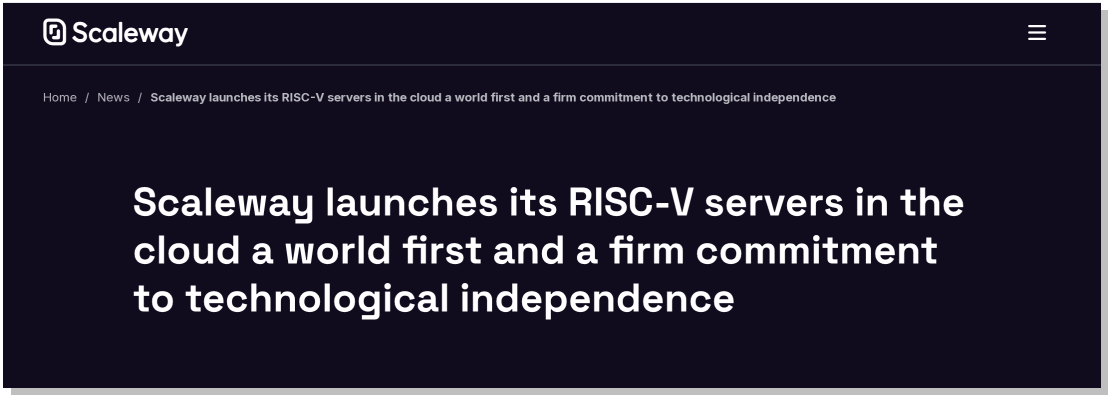
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

RISCover

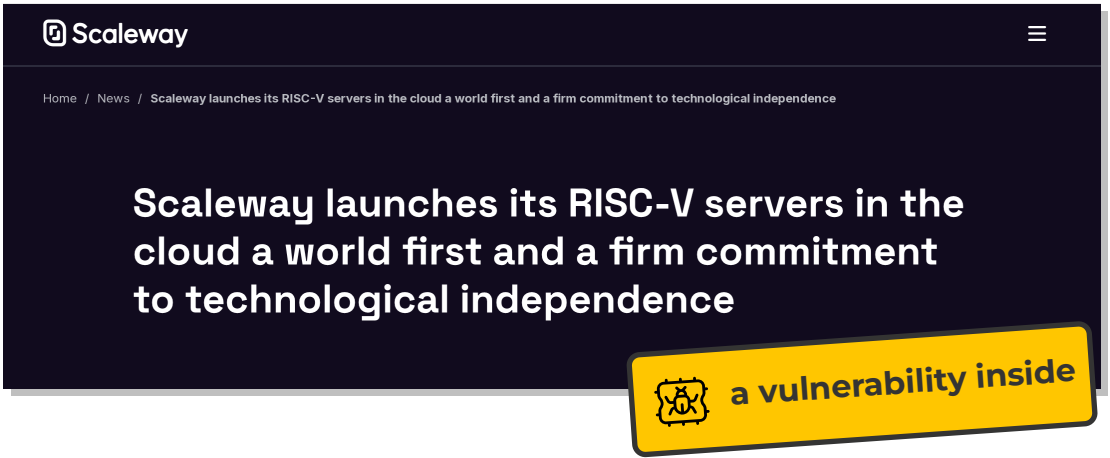
Automatic Discovery of User-exploitable Architectural Security Vulnerabilities in Closed-Source RISC-V CPUs

Fabian Thomas, Eric García Arribas, Lorenz Hetterich, Ruiyi Zhang, Daniel Weber, Lukas Gerlach, Michael Schwarz

Paris, France · Thursday, February 29, 2024



Paris, France · Thursday, February 29, 2024



Why Everyone Bets on RISC-V



arm



x86

Why Everyone Bets on RISC-V



open standard

Why Everyone Bets on RISC-V



open standard



no license fees



Why Everyone Bets on RISC-V



open standard



no license fees



extensible



Why Everyone Bets on RISC-V



open standard



no license fees



extensible

EU

€240 M funding

Why Everyone Bets on RISC-V



open standard



no license fees



extensible



EU

€240 M funding

China

national policy

Why Everyone Bets on RISC-V



open standard



no license fees



extensible



EU

€240 M funding

China

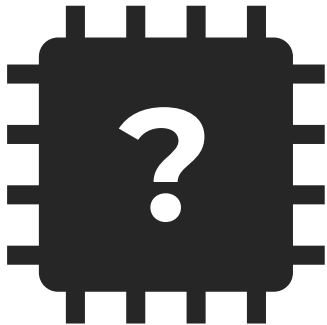
national policy

Scaleway

Open Standard, Closed Chips

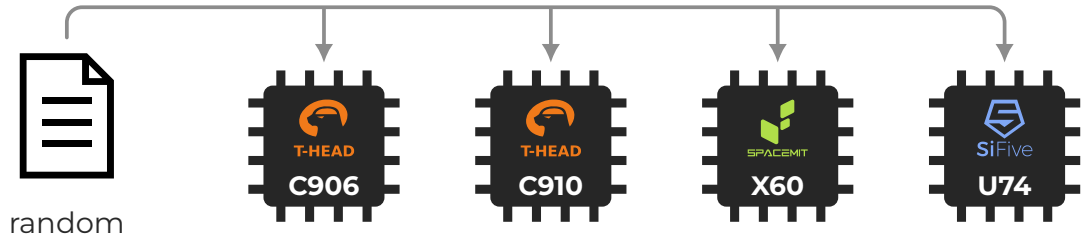
T-HEAD

Scaleway

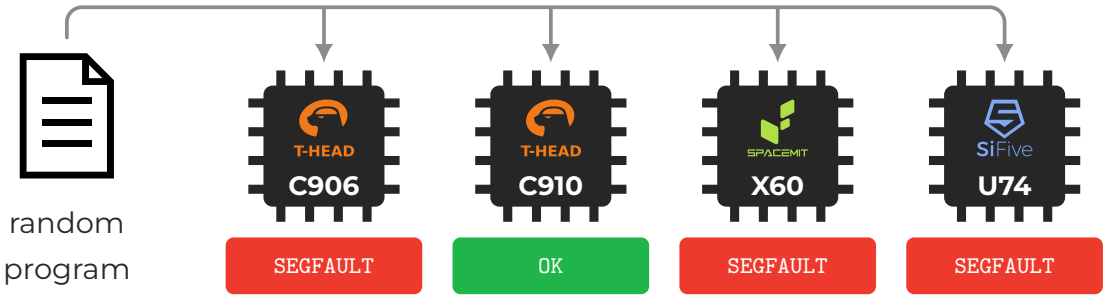


RISC-V

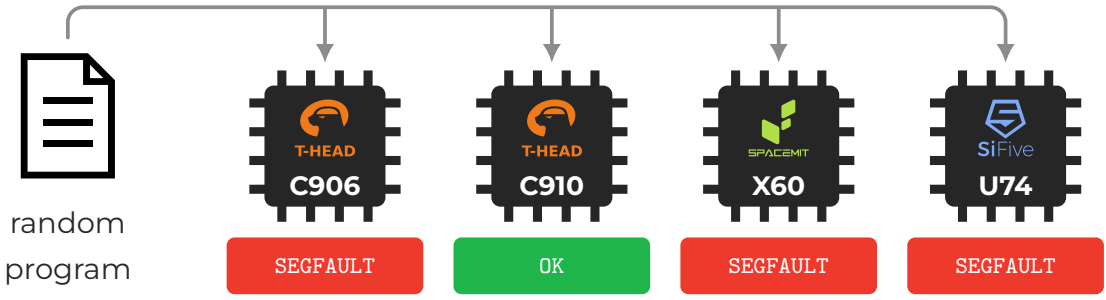
RISCover: Differential CPU Fuzzing



RISCover: Differential CPU Fuzzing



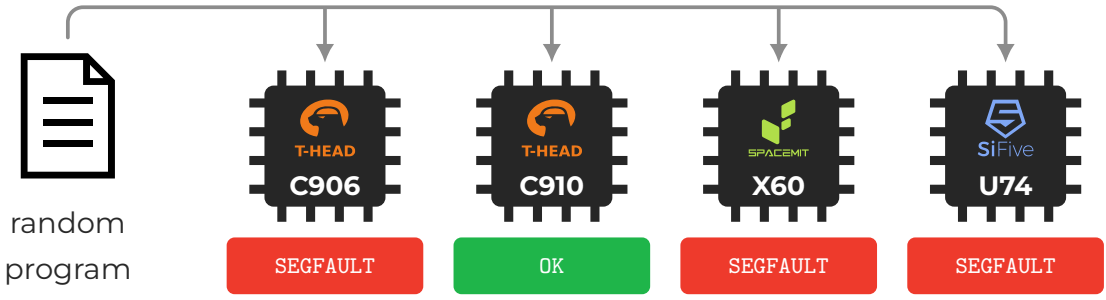
RISCover: Differential CPU Fuzzing



8

CPUs

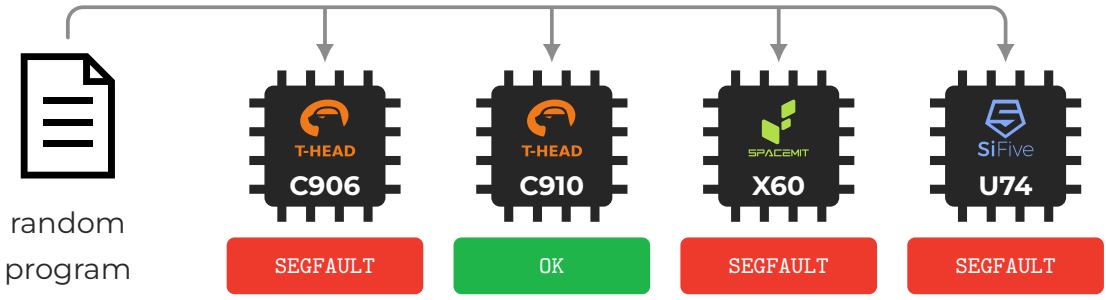
RISCover: Differential CPU Fuzzing



8 CPUs

3 vendors

RISCover: Differential CPU Fuzzing

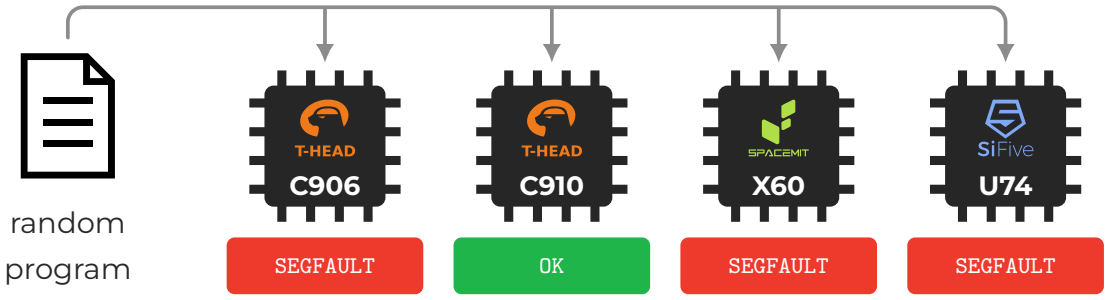


8 CPUs

3 vendors

4 vulnerabilities

RISCover: Differential CPU Fuzzing



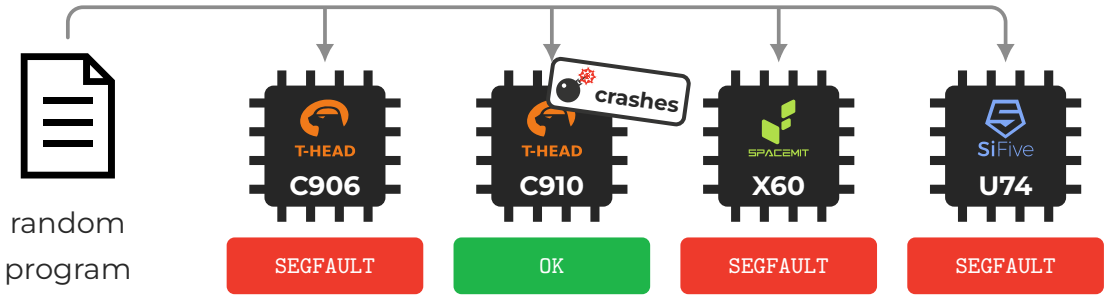
8 CPUs

3 vendors

4 vulnerabilities

seconds to find them

RISCover: Differential CPU Fuzzing



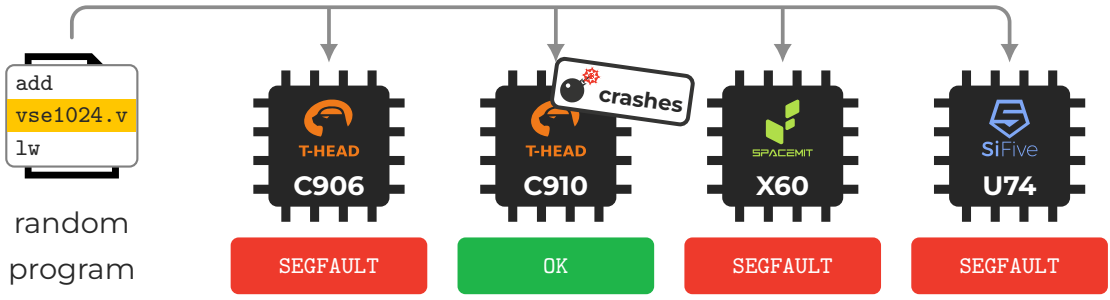
8 CPUs

3 vendors

4 vulnerabilities

seconds to find them

RISCover: Differential CPU Fuzzing



8 CPUs

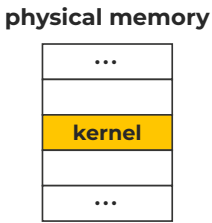
3 vendors

4 vulnerabilities

seconds to find them

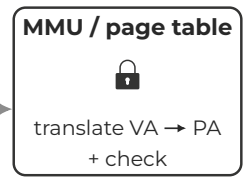
Memory Isolation

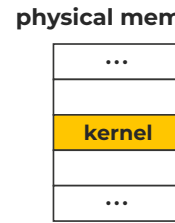
```
vse1024.v D, (A)
# store data D to
# virtual address A
```



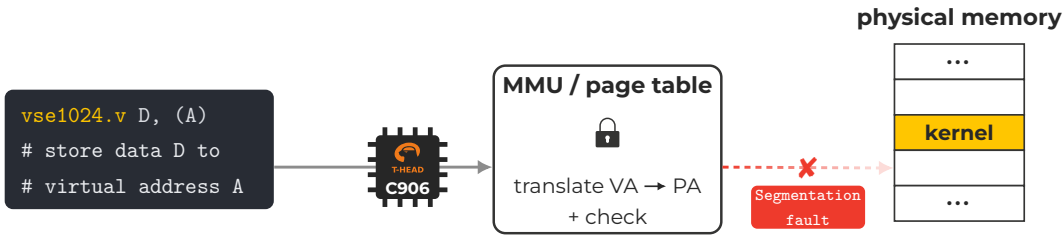
Memory Isolation

```
vse1024.v D, (A)
# store data D to
# virtual address A
```



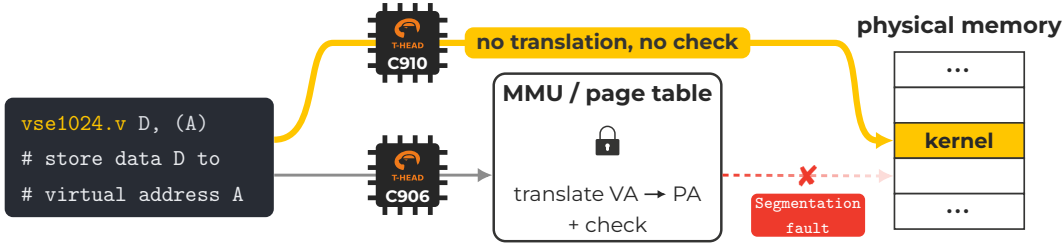


Memory Isolation



~~Memory Isolation~~: GhostWrite

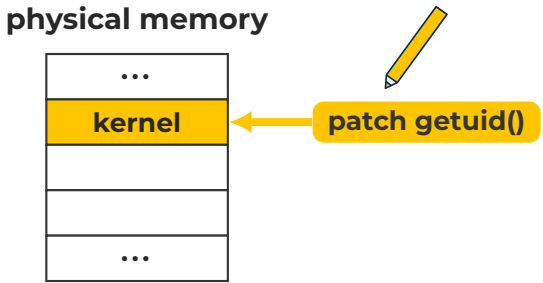
CVE-2024-44067



GhostWrite: Getting root

CVE-2024-44067

GhostWrite

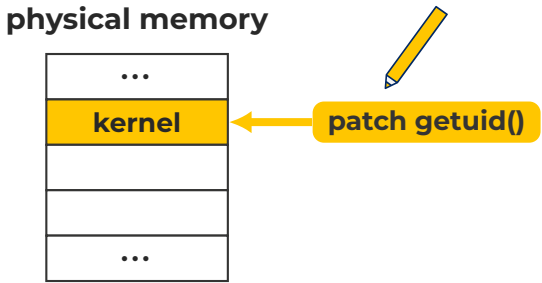



```
$ whoami
nobody
$ ./ghostwrite
```

GhostWrite: Getting root

CVE-2024-44067

GhostWrite

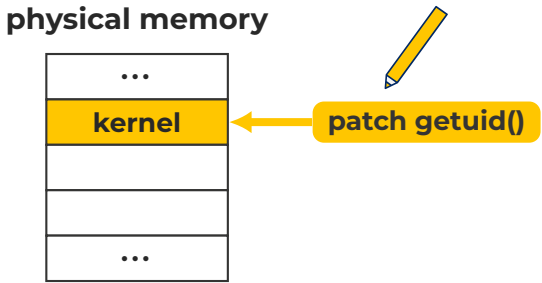



```
$ whoami
nobody
$ ./ghostwrite
$ whoami
root
```

GhostWrite: Getting root

CVE-2024-44067

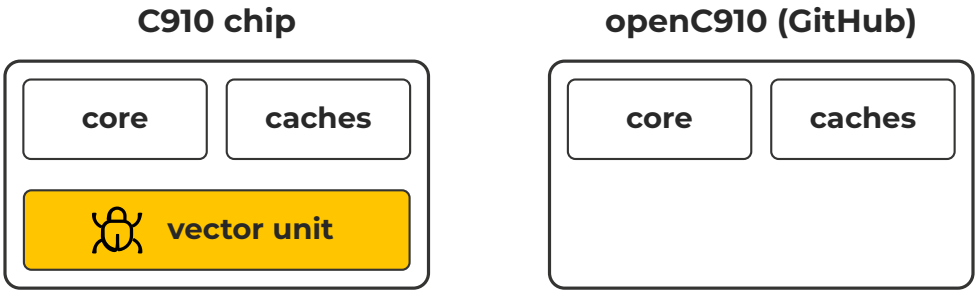
GhostWrite



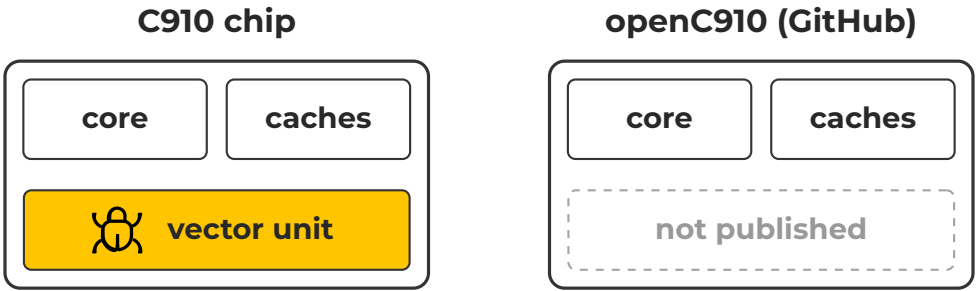
even from a container

```
$ whoami
nobody
$ ./ghostwrite
$ whoami
root
```

Silicon ≠ Published Code



Silicon ≠ Published Code



Unpatchable Silicon, Mitigated in Software



not software

fixed only in **new** chips

Unpatchable Silicon, Mitigated in Software



not software

fixed only in **new** chips



disable vector

≈ half of all instructions

Unpatchable Silicon, Mitigated in Software



not software

fixed only in **new** chips



disable vector

≈ half of all instructions

C910 board

```
$ lscpu
Vulnerabilities:
  Gather data sampling:  Not affected
  Ghostwrite:            Mitigation: xtheadvector disabled
  L1tf:                  Not affected
  Meltdown:              Not affected
```

Open standard ≠ open-source chips

Open-source code ≠ silicon

RISCover tests the silicon.



ghostwriteattack.com

github.com/cispa/RISCover

Open standard ≠ open-source chips

Open-source code ≠ silicon

RISCover tests the silicon.

Come to the poster:

→ reading **all memory**

→ **3 more vulnerabilities** that freeze CPUs



ghostwriteattack.com

github.com/cispa/RISCover