New issue

Jump to bottom

New transient execution attack on Boom. #577

Open JaewonHur opened this issue on Nov 8, 2021 · 0 comments

JaewonHur commented on Nov 8, 2021

Type of issue: bug report

Impact: rtl refactoring

Development Phase: proposal

Hi,
I found a new transient execution attack on risc-v boom.
The attack relies on the bug #558, which is a performance bug originally.
But the same bug can also be used to transiently poison the BIM table using a transiently accessed secret.

The attached PoC attack is a Meltdown type of attack where a supervisor-mode software transiently leaks a secret from the machine-mode software (i.e., either a firmware or an enclave).
The attack is based on two vulnerabilities: **1) boom transiently executes load instruction before checking PMP violation**, and **2) BIM table can be transiently updated using the accessed value**.
The attack is quite slow than using D-cache as a side channel, but it still works and almost correctly retrieves the secret value (i.e., *0xdeadbeef*).

- Used boom commit: `d77c2c3`
- How to reproduce the attack:

```
/* in the given directory */
make clean; make
<path to simulator-chipyard-SmallBoomConfig> ./exploit.riscv
```

This can be mitigated by fixing either one of two bugs above.

Template.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant