
CERN

Speculative Execution

What are the security vulnerabilities and how to mitigate them

Speculative Execution

- Shared principle:
  - Use speculative execution to bypass protections
  - Execution is reverted, but traces remain (CPU caches)

- Multiple naming conventions:
  - Google Project Zero: Variant 1/2/3
  - Press releases: Meltdown & Spectre
  - CVE-2017-{5753,5715, 5754}

- Our convention:
  - Spectre Variant 1 (CVE-2017-5753)
  - Spectre Variant 2 (CVE-2017-5715)
  - Meltdown/Variant 3 (CVE-2017-5754)

Spectre Variant 1

- Bounds Check Bypass
  - Bypass untrusted code execution restrictions
  - Kernel: eBPF JIT compiler
  - Browsers: JS engines
- Vulnerable: Intel, AMD, latest ARM
- Mitigations: add ‘LFENCE’ opcode
  - Kernel: fixed in latest kernel (reboot required)
  - Browsers: updates to limit attack efficiency
    - Google Chrome: enable “Site Isolation”

Spectre Variant 2

- Branch Target Injection:
  - Trick CPU to speculatively execute your code
  - Kernel, any userland program, **hypervisors**
- Vulnerable: Intel, (AMD)
- Mitigations:
  - IBRS: restrict/disable branch prediction
    - Microcode & kernel update required
    - “Userland protected” if ibrs_enabled set to 2
  - Retpoline: special construct to avoid issue (in dev)
    - New compiler option (GCC/LLVM)
    - Kernel/userland need to be patched & recompiled

Meltdown / Variant 3

- Rogue data cache load
  - Speculatively read kernel (protected) memory
- Vulnerable: Intel
- Mitigation: unmap kernel memory in userland
  - Fixed in latest kernel (KAISER / KPTI)
- Straight forward to abuse (lots of PoCs)
- Potential performance impact (syscalls)

What needs to be fixed, how:

- Variant 1 & 3 can be directly patched:
  - Only critical if untrusted/user code can run
- Variant 2:
  - Physical systems: requires microcode updates
  - VMs: requires:
    - kernel + microcode + qemu update on hypervisor
    - New QEMU process (hard-reboot) with correct CPU
- Patches are kernel related: reboot required!

Variant 2: microcode update?

- Initially only 3 Intel microcodes (1 AMD)
- Many more released by Intel Tuesday
  - RedHat update still pending
- Use script to check your hardware:
  - https://security.web.cern.ch/security/advisories/spectre-meltdown/spectre-cpu-microcode-checker.sh
  - /afs/cern.ch/user/v/vbrillau/public/spectre-cpu-microcode-checker.sh

www.cern.ch