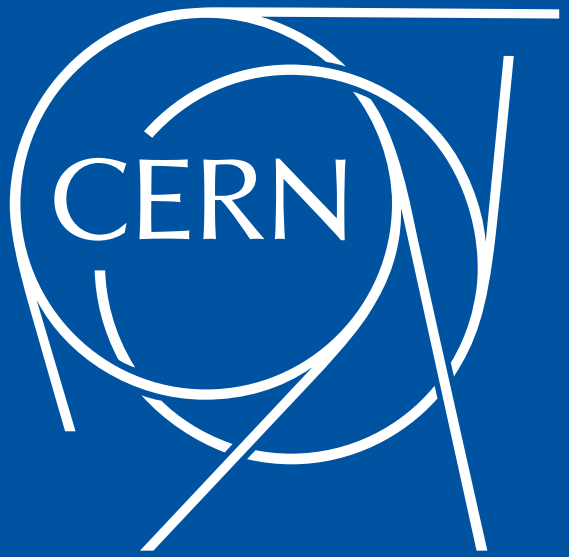
CERN

Spectre/meltdown vulnerabilities

Update on old and newly disclosed vulnerabilities & mitigation

Vincent Brillault

Variants 2: Updates in last months

`cat /sys/devices/system/cpu/vulnerabilities/spectre_v2`

- Retpoline:
  - Replaces IBRS (½ v2 microcode-based protection)
  - Only for CPU prior to Skylake (still using IBRS)
  - Affected: GCC (patch), kernel (recompiled)
  - Other packages only affected if updated/recompiled
- Microcode updates (Intel 20180425):
  - Adds IBRS support (for Skylake CPUs or old kernels)
  - Adds IBPB support (for full userland protection)
  - RHEL 6.x: Reboot or manual loading only
  - RHEL 7.x: Microcode loaded at update

→ Effect on performances, benchmarking?

RedHat: Microcodes

Policy clarification in recent vulnerability:

```
At this time, microprocessor microcode
will be delivered by the individual
manufacturers, but at a future time
Red Hat will release the tested and
signed updates as we receive them.
```

Variants 4: Speculative Store Bypass

```
cat /sys/devices/system/cpu/vulnerabilities/spec_store_bypass
```

- Discovered by Microsoft and Project Zero
  - Considered *low* risk by Microsoft
  - Project Zero PoC requires kernel patch to work
  - Considered *important* by RedHat, *high* by EGI
- Similar to v2, requires new microcode
  - Last public microcode release: April 25th
  - Beta versions sent to vendors: May 21st
  - Expected bios update: coming weeks
  - Expected firmware update (RHEL): future time...

→ Impossible to test/benchmark/deploy for now...


CERN