Spectre and Meltdown security vulnerabilities

- 3 variants: CVE-2017-5753, CVE-2017-5715, CVE-2017-5754
- All sites should install available packages as soon as possible
- Patched hosts need to be rebooted
- At this stage limiting user impact is recommended
- Early estimate: 1%-4% performance drop
- In case of virtualization, both hypervisor and VM must be patched
- CVE-2017-5715: “It’s complicated” – no updated microcode for some CPUs
  - Updated kernel must be used in conjonction with new microcode
  - https://cern.ch/security/advisories/spectre-meltdown/spectre-cpu-microcode-checker.sh
  - Situation complicated, changes every day
  - RedHat “microcode updates available”, then “talk to your OEM” after quality issues
  - Intel: “Sorry about the "higher system reboots” after applying firmware updates”
  - retpoline is a possible longer term alternative requiring no new microcode