# SUMMARY

of

# What we know about "Meltdown and Spectre"

Issued : 04/01/18 at 11h15 GMT+1 by Hacknowledge

## INTRODUCTION

- Vulnerabilities allowing unprivileged applications to access the current process or kernel memory (Meltdown) or other processes memory (Spectre)
- Vulnerabilities are using the processor L1 cache as an oracle to perform a side-channel attack to disclose content of the memory as such the vulnerabilities are in the processors themselves and not the software
- Vectors : unprivileged applications, guest hosts on paravirtualized systems, containers on Docker, LXC, OpenVZ, ... Patches from Microsoft, Mozilla and Chrome indicates than exploitation should also be possible from the browser through javascipt code
- Vulnerable systems: all OSes running on Intel CPU (Windows, Linux, *BSD, macOS, ...). Spectre also impact AMD and ARM processors
- Risks : access to secrets leading to elevation of privileges, access to sensitive information in the memory, bypass of protections against software exploitation techniques (*ASLR)

## DO 👍

- install the updates provided by your OS vendors when available
  - macOS 10.13.2 is already patched
  - a patch for the Linux kernel has been published but not yet available in distributions
  - Microsoft published patches for Edge (KB4056890) and for Windows (KB4056892)

- if running services on a hosted provider, contact them to know their status and actions
- if running services in the cloud (AWS, Azure, GCP, ...) follow their annoncements to know if patching will impact your services availability

## Sources


- https://googleprojectzero.blogspot.ch/2018/01/reading-privileged-memory-with-side.html
- https://support.microsoft.com/en-us/help/4056890/windows-10-update-kb4056890
- https://support.microsoft.com/en-us/help/4056892/windows-10-update-kb4056892
- https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html
- https://azure.microsoft.com/en-us/blog/securing-azure-customers-from-cpu-vulnerability/
- https://aws.amazon.com/security/security-bulletins/AWS-2018-013/


Hacknowledge