MELTDOWN & SPECTRE ADVISORY & FIXES 5TH JANUARY 2018

1. WHAT IS MELTDOWN & SPECTRE?

□ Meltdown: allow attackers to read physical memory (incl. kernel memory) from an unprivileged user process

□ Spectre: allows attacker to read memory from the current process only (not the kernel & other physical memory)

2. MELTDOWN ATTACK VECTORS

□ Privilege Escalation

- Attacker can execute a process they can dump most of the physical memory
- Might be able to retrieve password hashes, private keys etc.

□ Container / Paravirtualization Hypervisor Escape

- Targets kernel addresses that are shared between container & host kernel
- Attacker may leak data from the outside the container thus results to hypervisor escape

3. SPECTRE ATTACK VECTORS

□ Primary exploit scenario is ***JAVASCRIPT Execution***

□ Leak secret data from browser memory outside the Javascript sandbox

- Attacks could be used to leak browser cache or other saved data pertains to other site (ALWAYS LOGOUT. DON'T JUST PRESS "X")

□ Leaking addresses of user space modules to bypass ASLR (remote code execution)

- Attacks may crash the browser but data leakage is very limited
- Can also be used to determine the address of a module in memory & bypass ASLR

4. PATCHES & FIXES

□ **Microsoft**

- Windows 10 - KB4056892

  https://www.catalog.update.microsoft.com/Search.aspx?q=KB4056892
- Windows 7 & 8 patch will be released 9th January 2018 onwards
- IMPORTANT NOTE: IF YOU ARE USING 3RD PARTY AV ON THE SERVER/LAPTOP (APART FROM WINDOWS DEFENDER & SECURITY ESSENTIAL, KINDLY DISABLE THE AV BEFORE APPLYING THE PATCH. ELSE IT WON'T WORK)

□ **Apple macOS, iOS, tvOS, and Safari Browser**

- Update your IOS to version 11.2 or above
- Update your macOS to version 10.13.2 or above

- Update your tvOS to version 11.2 or above
- Safari Browser patch will be released soon in few days

□ **Android OS**

- Mobile OS updated on January 5th 2018 (apart of Android January Security Patch) are protected, according to Google (only for Google branded phone like Nexus / Pixel)
- Other Mobile Phones has to keep up to date on their manufacturer to release the patch. Turn on your Auto Update feature on your phone!

□ **Firefox Web Browser**

- Fixed version is 57.0.4 which solves both Meltdown and Spectre timing attacks

□ **Google Chrome Web Browser**

- Scheduled to release a patch for both vulnerabilities on January 23rd 2018 with the release of Chrome 64
- Meantime, users can enable an experimental feature called "Site Isolation" that can offer some protection against the web based exploits but might cause performance issue
  - ○ *Copy chrome://flags/#enable-site-per-process and paste it into the URL field at the top of your Chrome web browser, and then hit the Enter key.*
  - ○ *Look for Strict Site Isolation, then click the box labelled Enable.*
  - ○ *Once done, hit Relaunch Now to relaunch your Chrome browser.*

□ **Linux Distributions**

- The Linux kernel developers have also released patches for the Linux kernel with releases including versions 4.14.11, 4.9.74, 4.4.109, 3.16.52, 3.18.91 and 3.2.97, which can be downloaded from Kernel.org.

□ **VMWare & Citrix**

- VMWare has released their patch to address this issue

  https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html

- Citrix did not release any security patches to address the issue but guided it's customer and recommended them to check for any update on relevant 3rd party software

  https://support.citrix.com/article/CTX231399