Virtual Machines with side channel mitigations enabled may exhibit performance degradation (79832)

https://kb.vmware.com/s/article/79832

Last Updated: 11/18/2021**Categories:** Informational**Total Views:** 418816

Symptoms

Virtual Machines that have side channel mitigations enabled while running on Fusion on Mac OS 11.0 or later or on Workstation on Windows hosts with virtualization based security enabled may run slowly.

Cause

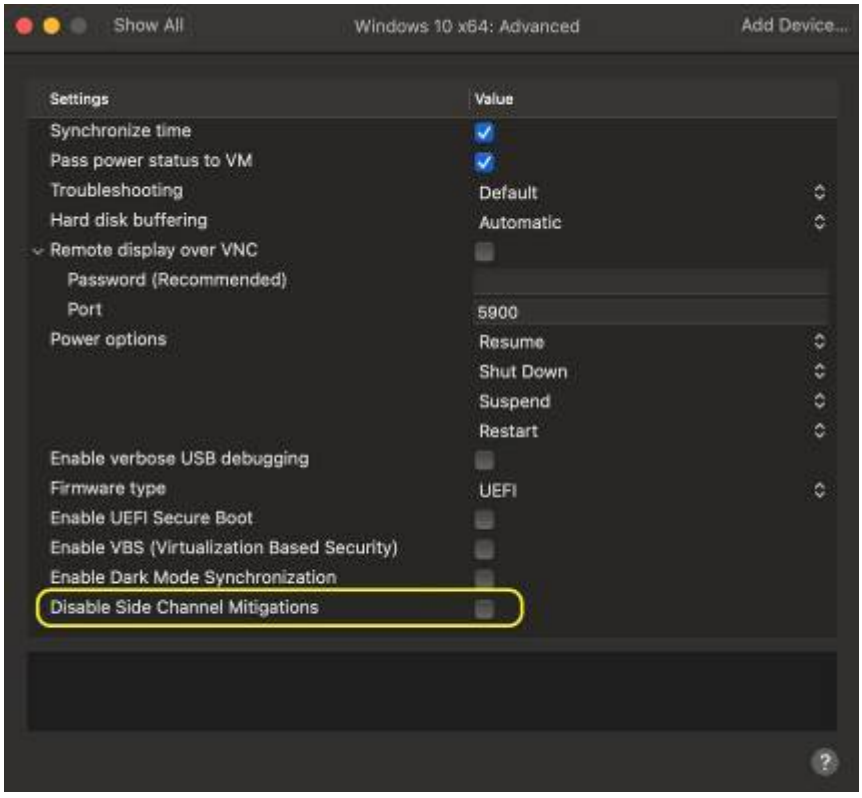
The root cause of the performance degradation is most likely due to mitigations for side channel attacks such as Spectre and Meltdown. Side channel attacks allow unauthorized read access by malicious processes or virtual machines to the contents of protected kernel or host memory. CPU vendors have introduced a number of features to protect data against this class of attacks such as indirect branch prediction barriers, single thread indirect branch predictor mode, indirect branch restricted speculation mode and L1 data cache flushing. While these features are effective at preventing side channel attacks they can cause noticeable performance degradation in some cases.
Resolution

The process to Disable Side Channel Mitigations:

To disable side-channel mitigations use the Workstation Pro / Fusion UI.

On Fusion:

- Start Fusion
- Virtual Machine should be Shut Down
- Go to Virtual Machine > Settings > Advanced
- Check "Disable Side Channel Mitigations"



On Workstation Pro:

- Start Workstation
- Virtual Machine should be Shut Down
- Go to `VM > Settings > Options > Advanced`
- Check "Disable Side Channel Mitigations for Hyper-V enabled hosts"

Note: Above settings are not applicable in VMware Workstation Player