



Forum: Sécurité

Topic: Performances suite mise à jour faille processeur Intel

Subject: Re: Performances suite mise à jour faille processeur Intel

Publié par: Tof81

Contribution le : 13/01/2018 16:25:36

J'ai oublié de mettre dans mon post #26 où je presentais les résultats des tests de vitesse après avoir comblé complétement les failles, les résultats de SpecuCheck (voir post #23).

Fichier(s) attaché(s):

SpecuCheck.jpg (38.46 KB)

```
SpecuCheck v1.0.5 -- Copyright(c) 2018 Alex Ionescu
https://ionescu007.github.io/SpecuCheck/ -- @aionescu
-----
Mitigations for CVE-2017-5754 [rogue data cache load]
-----
[-] Kernel VA Shadowing Enabled: yes
  └─> with User Pages Marked Global: no
  └─> with PCID Flushing Optimization (INVPCID): yes
-----
Mitigations for CVE-2017-5715 [branch target injection]
-----
[-] Branch Prediction Mitigations Enabled: yes
  └─> Disabled due to System Policy (Registry): no
  └─> Disabled due to Lack of Microcode Update: no
[-] CPU Microcode Supports SPEC_CTRL MSR (048h): yes
  └─> Windows will use IBRS (01h): yes
  └─> Windows will use STIPB (02h): yes
[-] CPU Microcode Supports PRED_CMD MSR (049h): yes
  └─> Windows will use IBPB (01h): yes
```