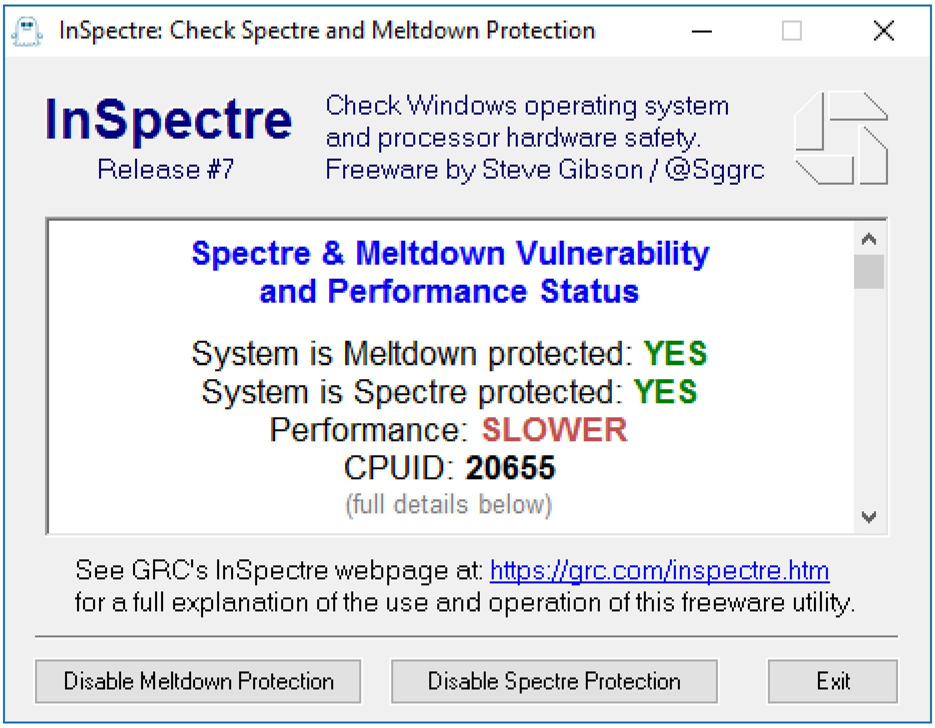
JACKSOFT LABS

R1170Y8 & R0300Y8 MELTDOWN/SPECTRE PATCH

Update x2: August Microcodes

All you know what happened with Intel security last months and I'll be short with this post.
Thanks to Win-Raid Forum I obtained new CPU microcodes (unofficially released yet on Intel website, maybe not fully tested, but signed as PRODUCT, so they should be reliable) and new ME Firmware (with updater!) and made a new release of the R1170Y8 BIOS for VPCEB4C5E.



InSpectre: Check Spectre and Meltdown Protection

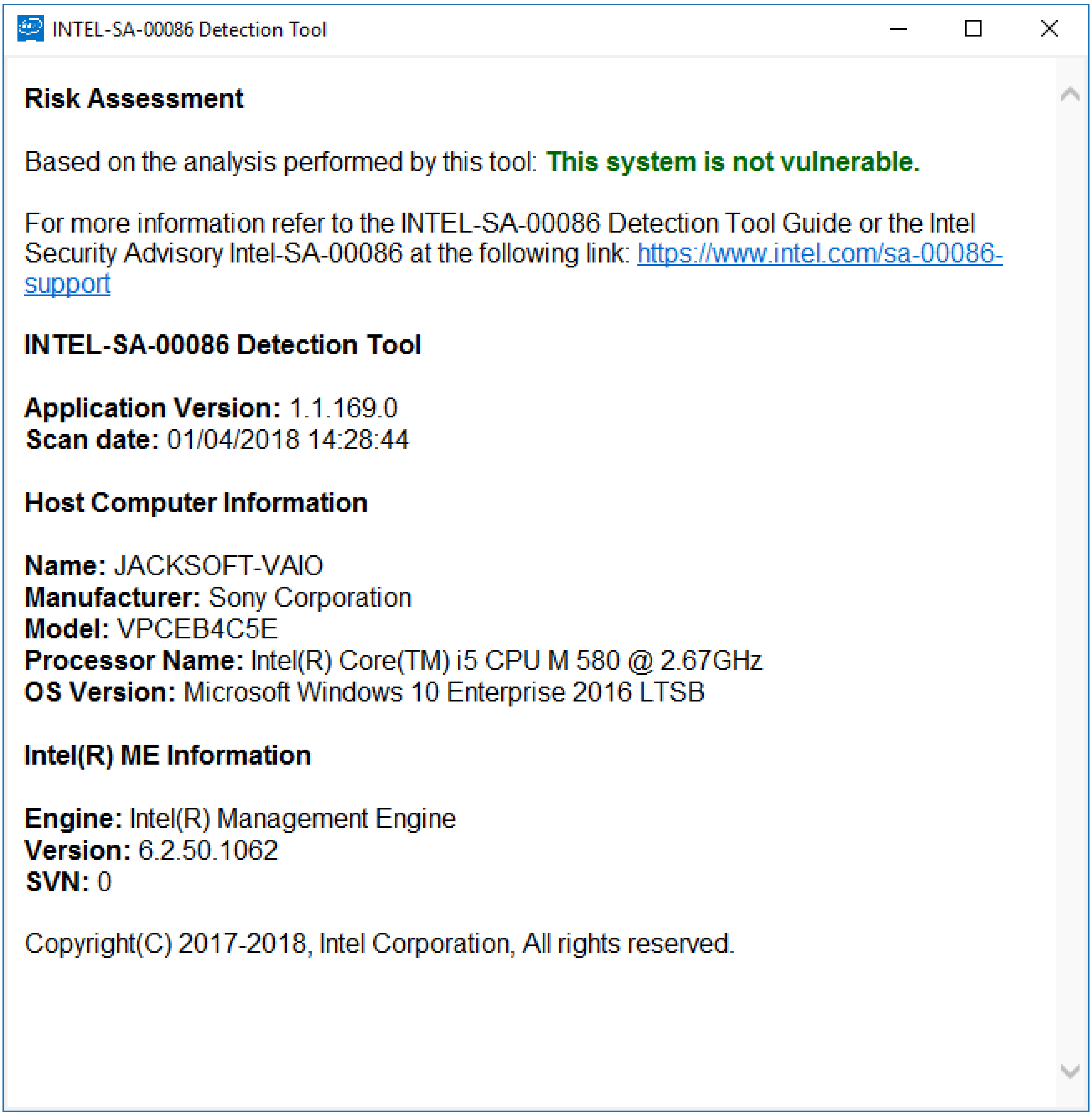
InSpectre
Release #7

Check Windows operating system and processor hardware safety.
Freeware by Steve Gibson / @Sggrc

Spectre & Meltdown Vulnerability and Performance Status

System is Meltdown protected: YES
System is Spectre protected: YES
Performance: SLOWER
CPUID: 20655
(full details below)

See GRC's InSpectre webpage at: https://grc.com/inspectre.htm
for a full explanation of the use and operation of this freeware utility.



Risk Assessment

Based on the analysis performed by this tool: **This system is not vulnerable.**

For more information refer to the INTEL-SA-00086 Detection Tool Guide or the Intel Security Advisory Intel-SA-00086 at the following link: https://www.intel.com/sa-00086-support

INTEL-SA-00086 Detection Tool

Application Version: 1.1.169.0
Scan date: 01/04/2018 14:28:44

Host Computer Information

Name: JACKSOFT-VAIO
Manufacturer: Sony Corporation
Model: VPCEB4C5E
Processor Name: Intel(R) Core(TM) i5 CPU M 580 @ 2.67GHz
OS Version: Microsoft Windows 10 Enterprise 2016 LTSB

Intel(R) ME Information

Engine: Intel(R) Management Engine
Version: 6.2.50.1062
SVN: 0

Copyright(C) 2017-2018, Intel Corporation, All rights reserved.

NB: To make sure protection works Windows MUST be updated to the latest availables security patches on Windows Update!
Of course if newer CPU microcodes and ME firmwares will be released I'll update this post ASAP.

IMPORTANT: Before flash, check which BIOS version you have. To check this: shutdown your laptop, power it on and press immediately and repeatedly "F2" button on keyboard, you'll enter in the BIOS menu. Read "BIOS Version" and check if it's "R1170Y8". If your BIOS IS NOT named as these DON'T GO FORWARD! DO NOT FLASH ANYTHING!!!

To prevent any problem close all programs, and also disable the antivirus. Some programs can interfere with the BIOS flash and in result you can BRICK your machine!

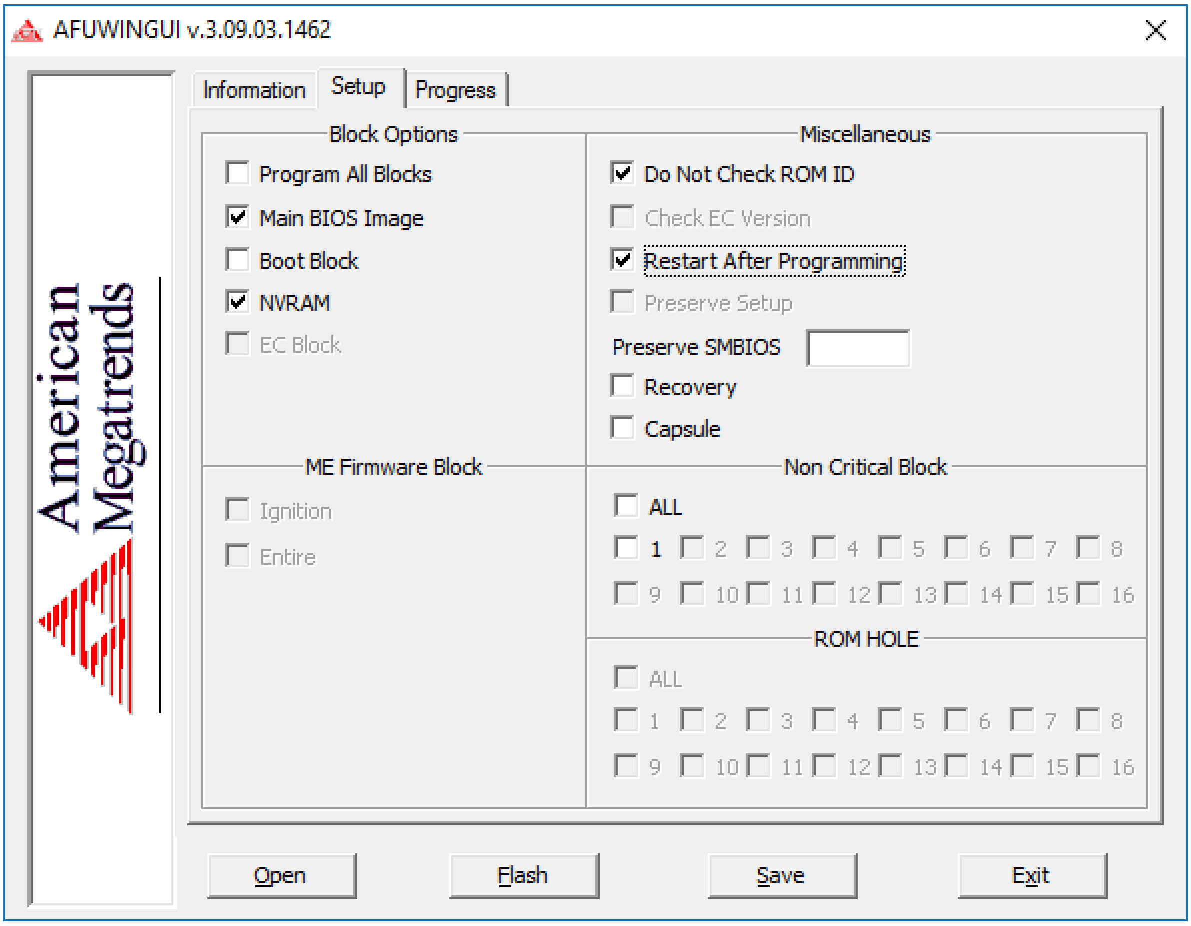
Note: You'll hear the fan spinning to the maximum speed and in some operation (read or write) your mouse and keyboard will be temporarily disabled, this is normal.

Open AfuWin (select 32 or 64bit, depends on your OS), and first make a backup of your current ROM by clicking on the “Save” button. Write a name for your BIOS (eg. my_bios_ok.rom), if you want, and save in a known location to easily retrieve it if you need to. Be sure to make multiple copies of this backup (on external drive like USB pendrives, etc).
WARNING: This updates are EXPERIMENTAL! This means that you COULD BRICK. Make sure you have a way to recover your original full BIOS (ME+BIOS) with an SPI dump!

Since I had just one freeze during stress tests with August microcodes I decided to not remove links to previous version, in case you need to downgrade. At least for now.

PS: Now Intel declared our CPUs as Legacy :P
– Removed all engineering CPU microcodes (they’re pretty useless unless you have an engineering sample CPU…)
– Updated existent CPU microcodes to latest available version taken from Win-Raid.

Use AfuWin to update with the same parameters as in the screenshot below:



Block Options
☐ Program All Blocks
☑ Main BIOS Image
☐ Boot Block
☑ NVRAM
☐ EC Block

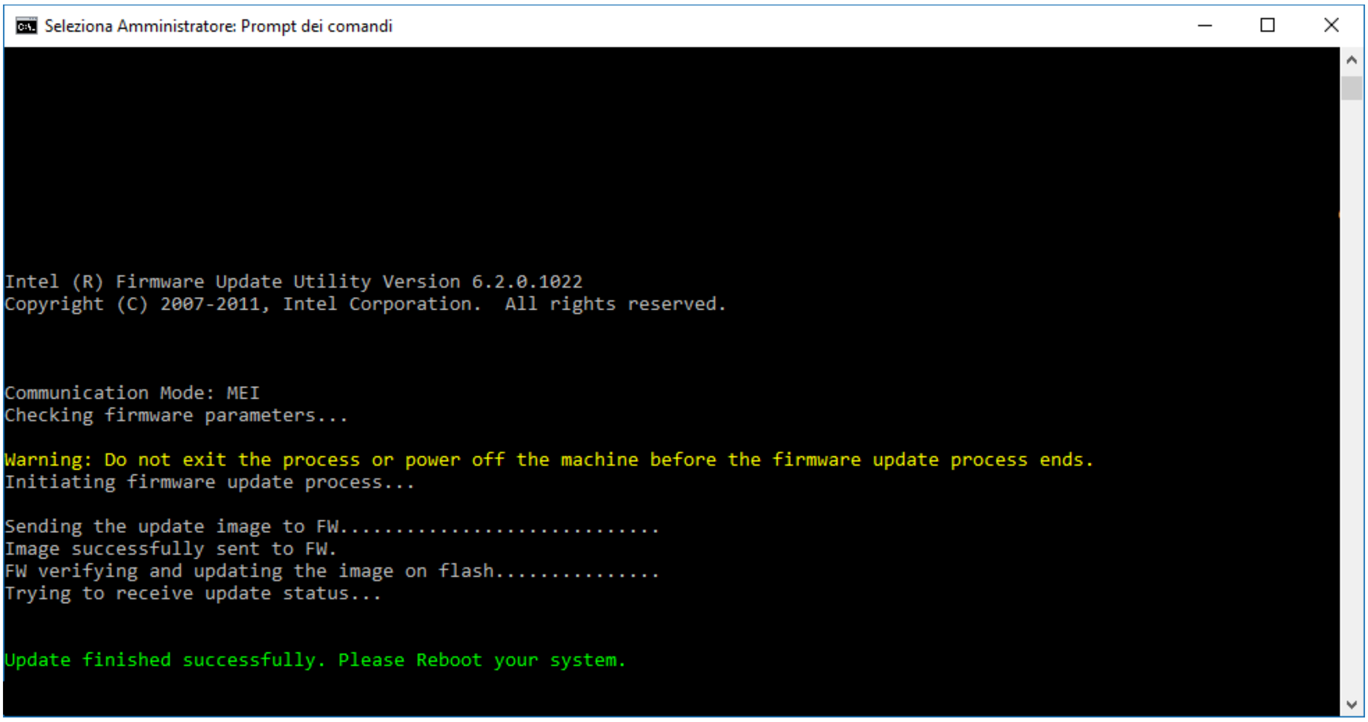
ME Firmware Block
☐ Ignition
☐ Entire

Miscellaneous
☑ Do Not Check ROM ID
☐ Check EC Version
☑ Restart After Programming
☐ Preserve Setup
Preserve SMBIOS
☐ Recovery
☐ Capsule

Non Critical Block
☐ ALL
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8
☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16

ROM HOLE
☐ ALL
☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8
☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16

– Update to 6.2.50.1062, use the batch “update”, as admin, to start the updater, if not works use this command as admin “FWUpdLcl.exe 6.2.50.1062_1.5MB_PRD_UPD.bin -generic” (without quotes).



```
Intel (R) Firmware Update Utility Version 6.2.0.1022
Copyright (C) 2007-2011, Intel Corporation.  All rights reserved.


Communication Mode: MEI
Checking firmware parameters...

Warning: Do not exit the process or power off the machine before the firmware update process ends.
Initiating firmware update process...

Sending the update image to FW............................
Image successfully sent to FW.
FW verifying and updating the image on flash..............
Trying to receive update status...


Update finished successfully. Please Reboot your system.
```

Since there was some discussion about performance drops after microcodes patch I made some benchmark before and after the patch, and here are the results:

As you can see the performance drop is really low, and maybe they also depends on some Windows updates too. The hardware used is the current:

VAIO VPCEB4C5E: Modded R1170Y8 BIOS v0.4-v0.5 / Intel Core i5 580M / ATI Radeon HD5650 1GB / 2x4GB Crucial RAM 1333MHz CL10 @ 1066MHz CL7 / 256GB Crucial M4 SSD / 1920x1080p internal display.

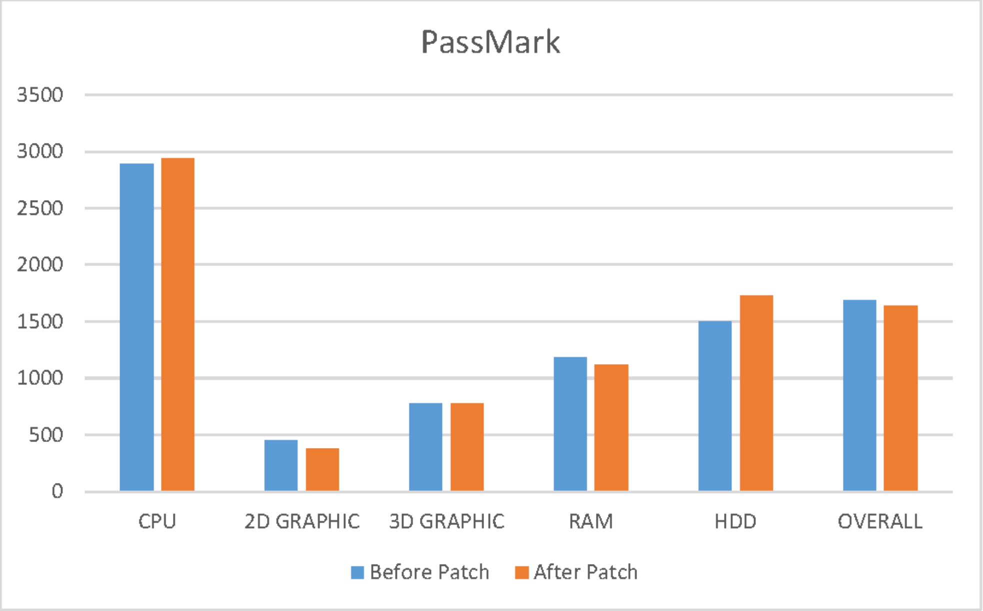
Software used: Windows 10 Enterprise LTSB 2016 / PassMark Performance Test 9.0.1023 (Trial) / 3DMark Basic Edition

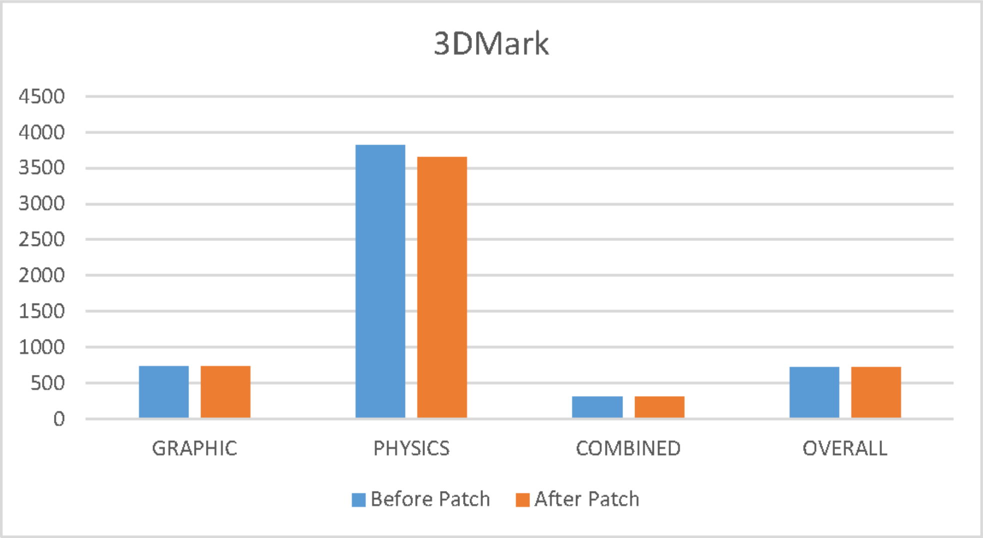
PassMark

TEST	CPU	2D GRAPHIC	3D GRAPHIC	RAM	HDD	OVERALL
Before Patch	2890,1	452,3	775,1	1184,4	1496,6	1689,2
After Patch	2937,6	383,5	773,8	1117,2	1727,6	1641
Difference	1,63%	-16,46%	-0,17%	-5,84%	14,33%	-2,89%

3D Mark

TEST	GRAPHIC	PHYSICS	COMBINED	OVERALL
Before Patch	728	3821	311	718
After Patch	727	3657	311	717
Difference	-0,14%	-4,39%	0,00%	-0,14%





WARNING, I'LL NOT ASSUME ANY RESPONSIBILITY ABOUT THIS ARTICLE AND FILES/SOFTWARE LINKED, PUBLICIZED AND MENTIONED HERE! BIOS MODDING IS REALLY DANGEROUS AND COULD BRICK OR DAMAGE YOUR MACHINE! BE SURE TO KNOW WHAT ARE YOU DOING AND POSSIBLY HAVE AN SPI DUMP OF YOUR FULL BIOS!!!