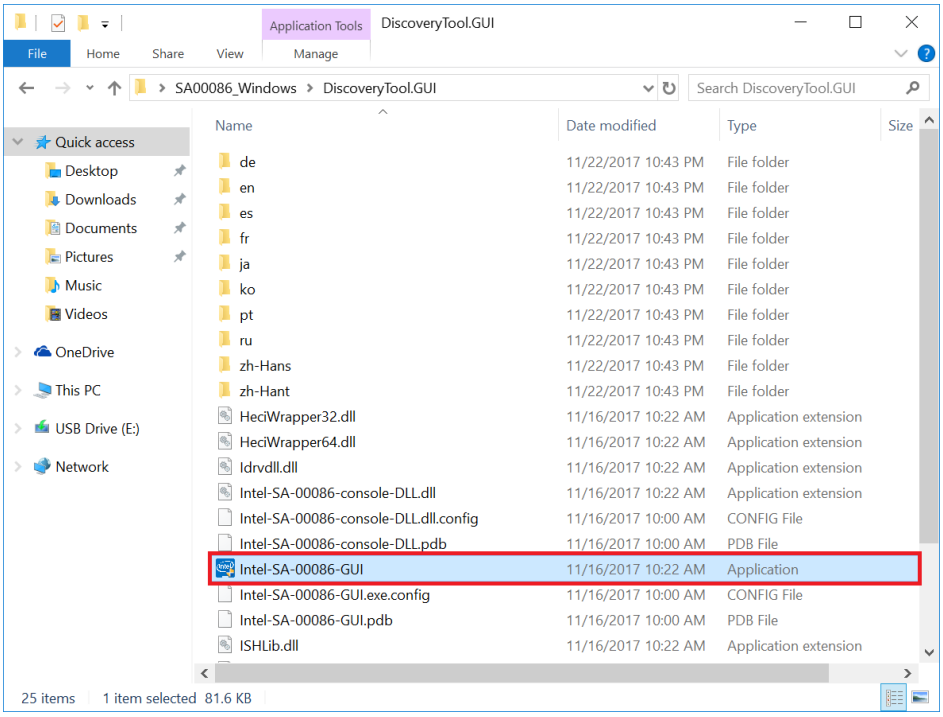
Intel ME Security Vulnerabilities (Intel SA-00086) Firmware Update Guide

Prepared by MSI NB FAE Team | Revision: 1.0 | Date: 2017 / 11 / 30

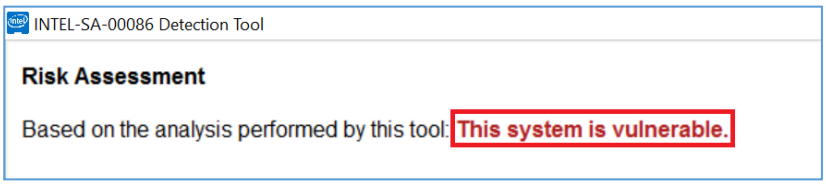
The Intel ME Update Tool is to patch the security vulnerabilities (Intel SA-00086[1]) which Intel identified and applies to MSI Notebook, Vortex and VR ONE which bundled with the 6th, 7th and 8th generation Intel® Core Processor which has specific Intel ME Firmware versions 11.0/11.5/11.6/11.7/11.10/11.201 only.

A. Check if the ME firmware update is needed

1. Download the Intel-SA-00086 Detection Tool[2].
2. Extract the file on the desktop and enter the file “DiscoveryTool.GUI”.
3. Double click on “Intel-SA-00086-GUI.exe” run the detection tool.



4. If the result “This system is vulnerable.” shows after the risk assessment complete, continue the ME firmware update.



B. Download and Update BIOS to the latest version released on MSI website.

To keep a stabled system environment, make sure to have the latest BIOS updated before the ME firmware update.

5. Download and update the latest BIOS.
6. Reboot the system and press “Delete” button to enter the BIOS menu.
7. Load the optimized default settings and save the configurations by pressing F9 and F10.

*1 Intel ME 11.x Security Review Cumulative Update

*2 Intel-SA-00086 Detection Tool

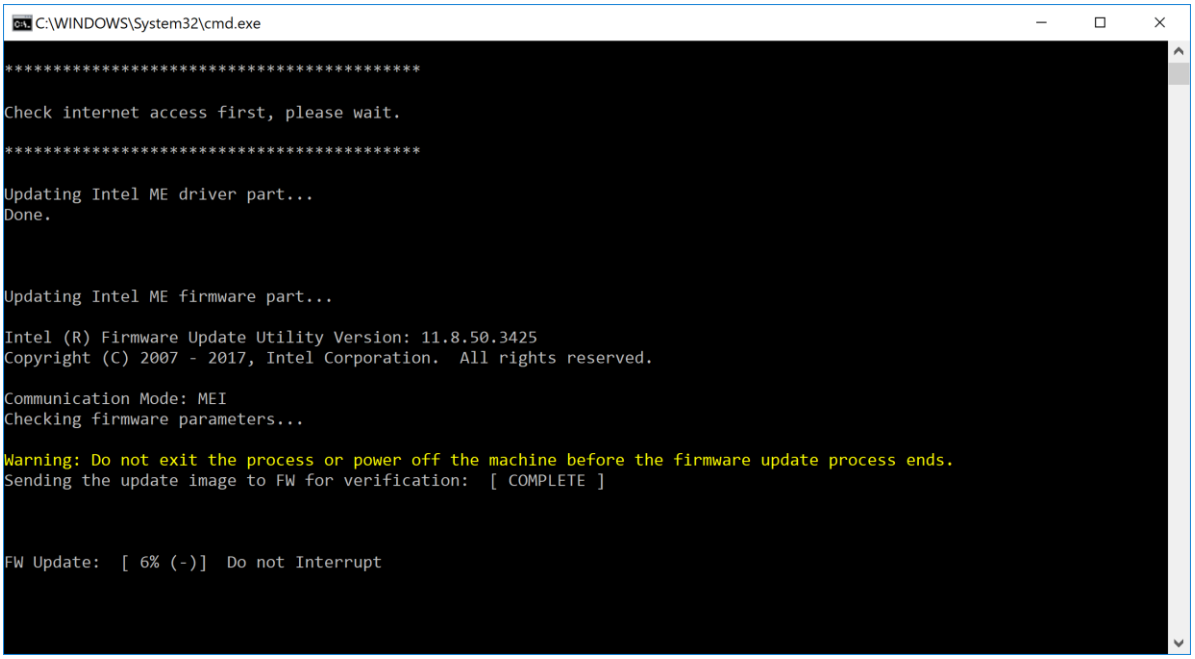
C. Update Intel ME Firmware

The update has two parts, first updating the ME driver and then continue with the ME firmware update.

CAUTION

Make sure to keep the network connection during the whole update process.

8. Download the ME Update Tool from the BIOS download page.
9. Extract the ME Update Tool “ME118H” on the desktop.
10. Double click on the batch file “ME118H.bat” to start the update.
    (The update process takes 5 to 10 mins)



11. The system restarts automatically after the firmware update complete.

D. Confirm the Security Vulnerabilities has been patched

12. Run the Intel-SA-00086 Detection Tool again.
13. The assessment result should now shows “This system is not vulnerable. It has already been patched.” or “The system is not vulnerable”.