



How to patch Intel
security vulnerabilities
(SA-00086) by M-flash
function for Pro series.



SOME ARE PC, WE ARE GAMING

TRUE **G**AMING



msi

What is Intel security
vulnerabilities (SA-
00086)

What is Intel security vulnerabilities (SA-00086)

Description:

- In response to issues identified by external researchers, Intel has performed an in-depth comprehensive security review of its Intel® Management Engine (ME), Intel® Trusted Execution Engine (TXE), and Intel® Server Platform Services (SPS) with the objective of enhancing firmware resilience.
- <https://security-center.intel.com/advisory.aspx?intelid=intel-sa-00086&languageid=en-fr>

Please follow step for patch it

- Step A: Check this BIOS is for Intel-SA-00086 or latest and then flash BIOS by M-flash function under Pro series system.

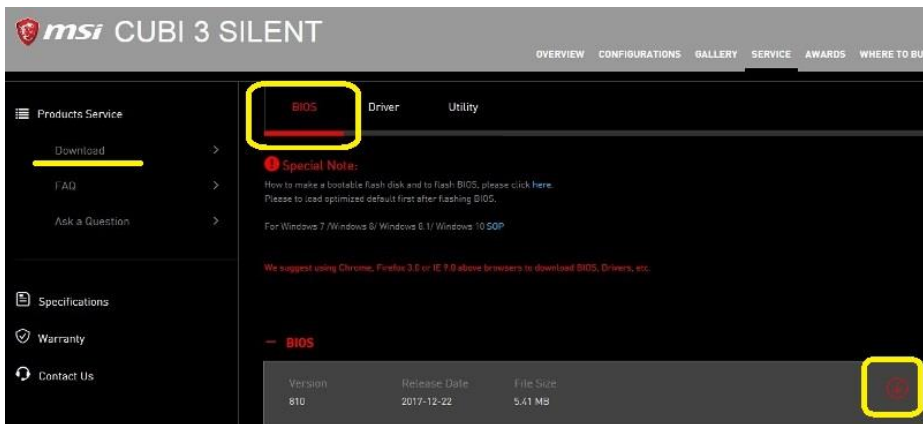
Note: Flash BIOS will be also update ME version by M-flash function.

- Step B: Use Intel-SA-00086 Detection Tool for checking again.

Note: If still, please connect with internet and the reboot it again.

Step A-1 Copy BIOS file to USB flash drive

- Prepare an USB or portable storage device.
- Download and unzip the BIOS files from MSI webpage. (There is a Special Note for updating BIOS under Dos mode for reference.)
- Copy the BIOS file into your device directory(root). As the picture below, there is only one file you have to copy.



Step A-2 Into BIOS setup

- Reboot / Turn on your computer, hitting the Del key when the boot screen shows up. You will get into the BIOS configuration screen.



Step A-3 Flash BIOS by M-flash function

- Check the current BIOS version is v807.



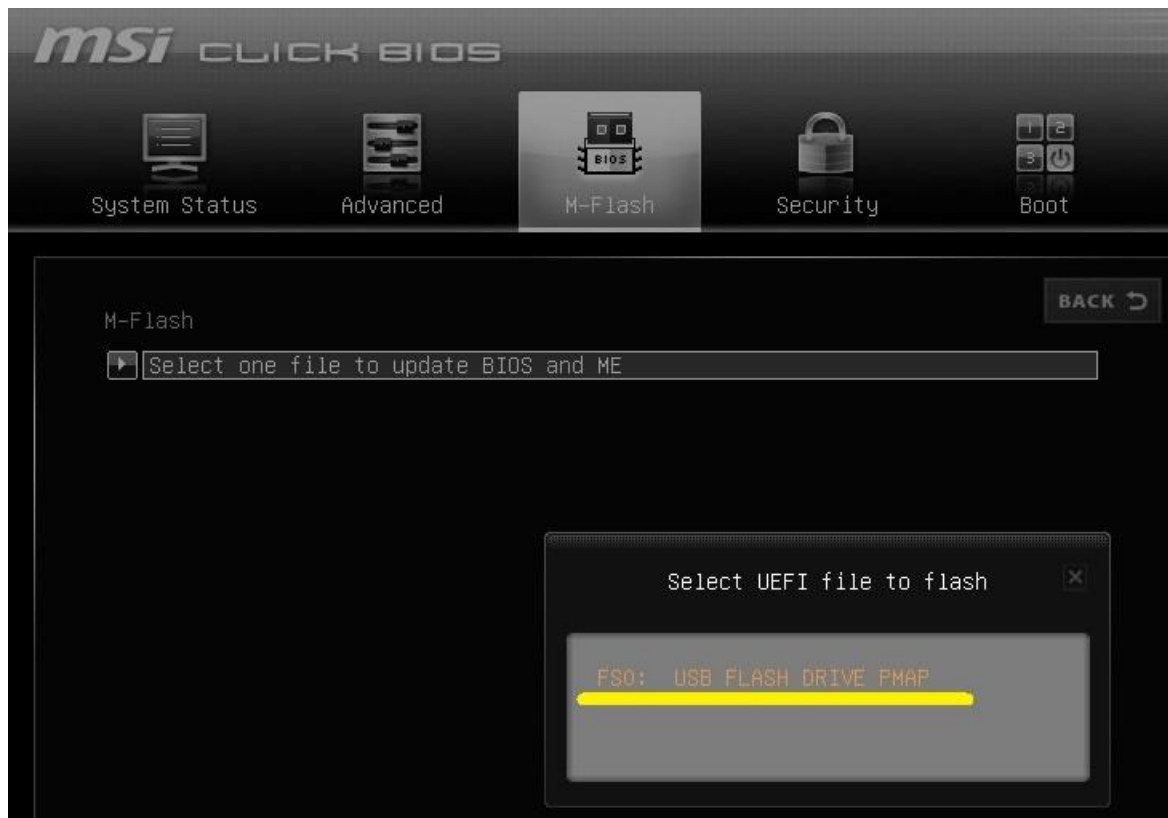
Step A-4 Flash BIOS by M-flash function

- Into M-FLASH screen.
- Select one file to update BIOS and ME.



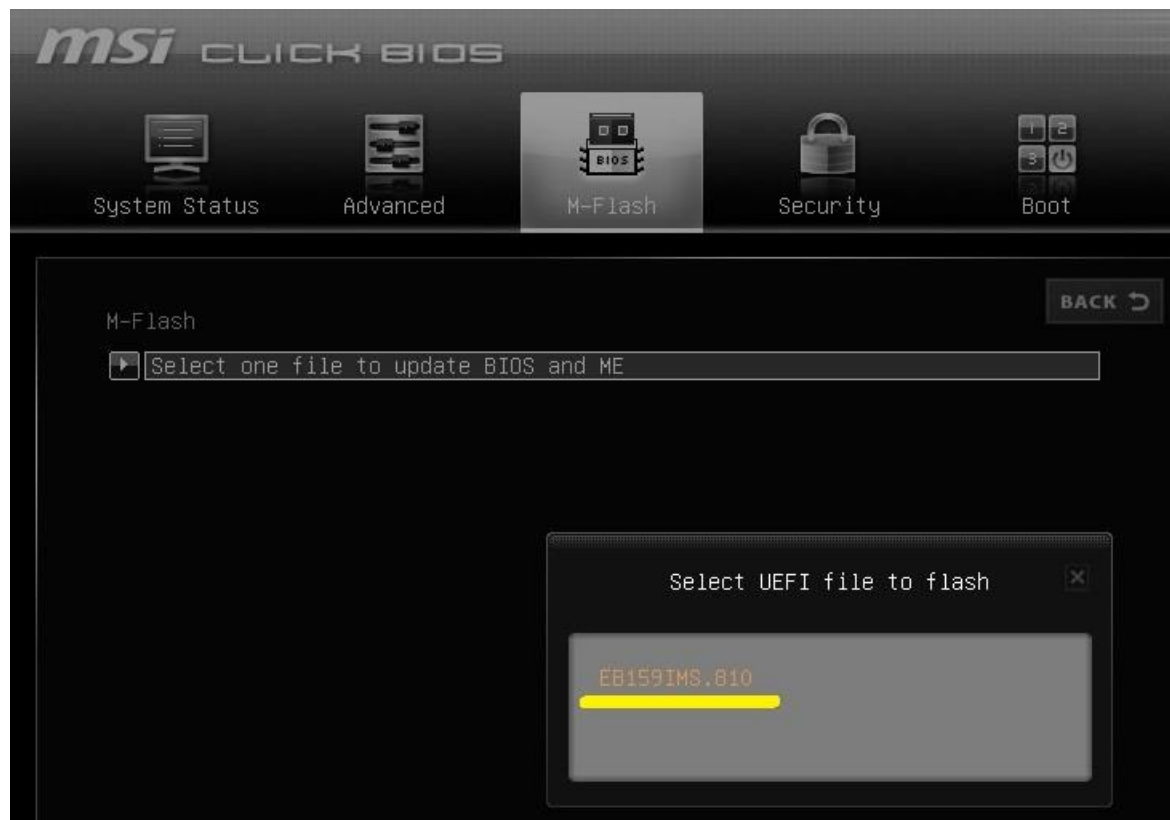
Step A-5 Flash BIOS by M-flash function

- Select USB flash drive.



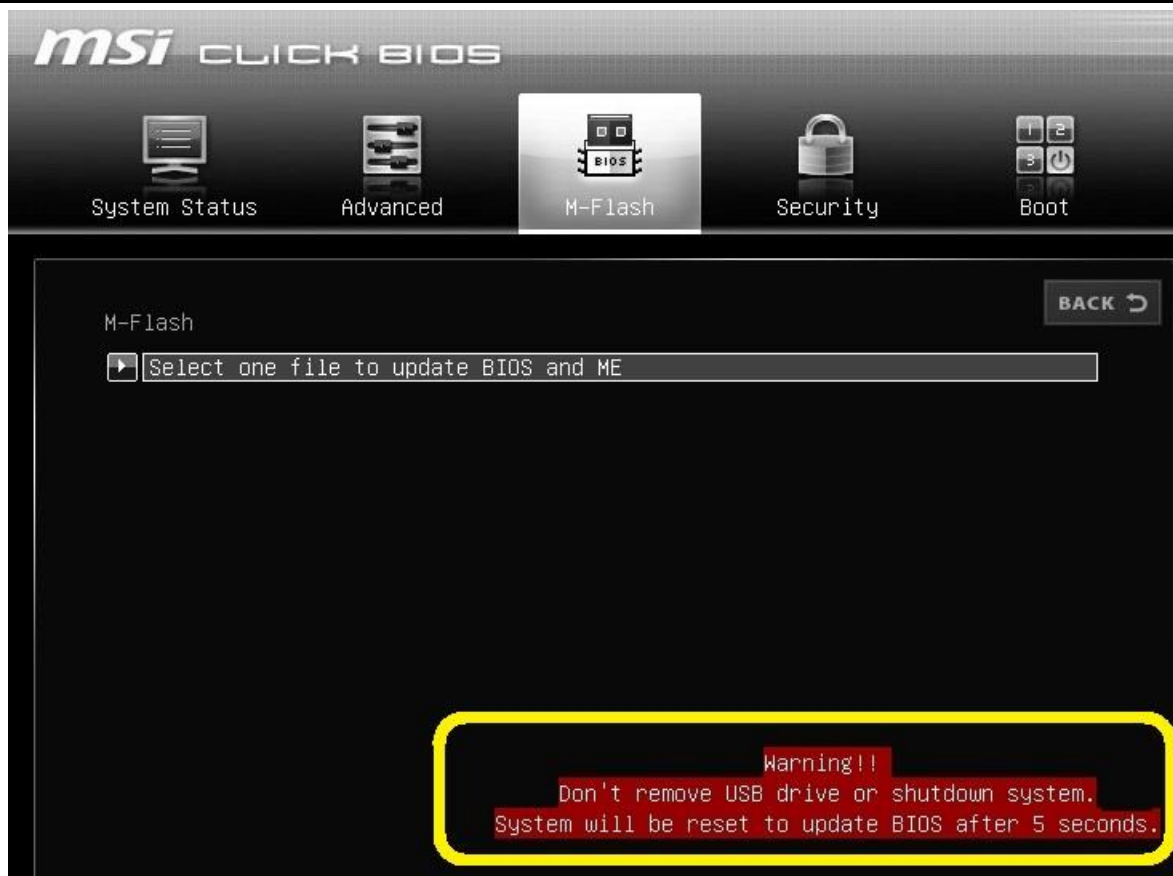
Step A-6 Flash BIOS by M-flash function

- Select BIOS file.



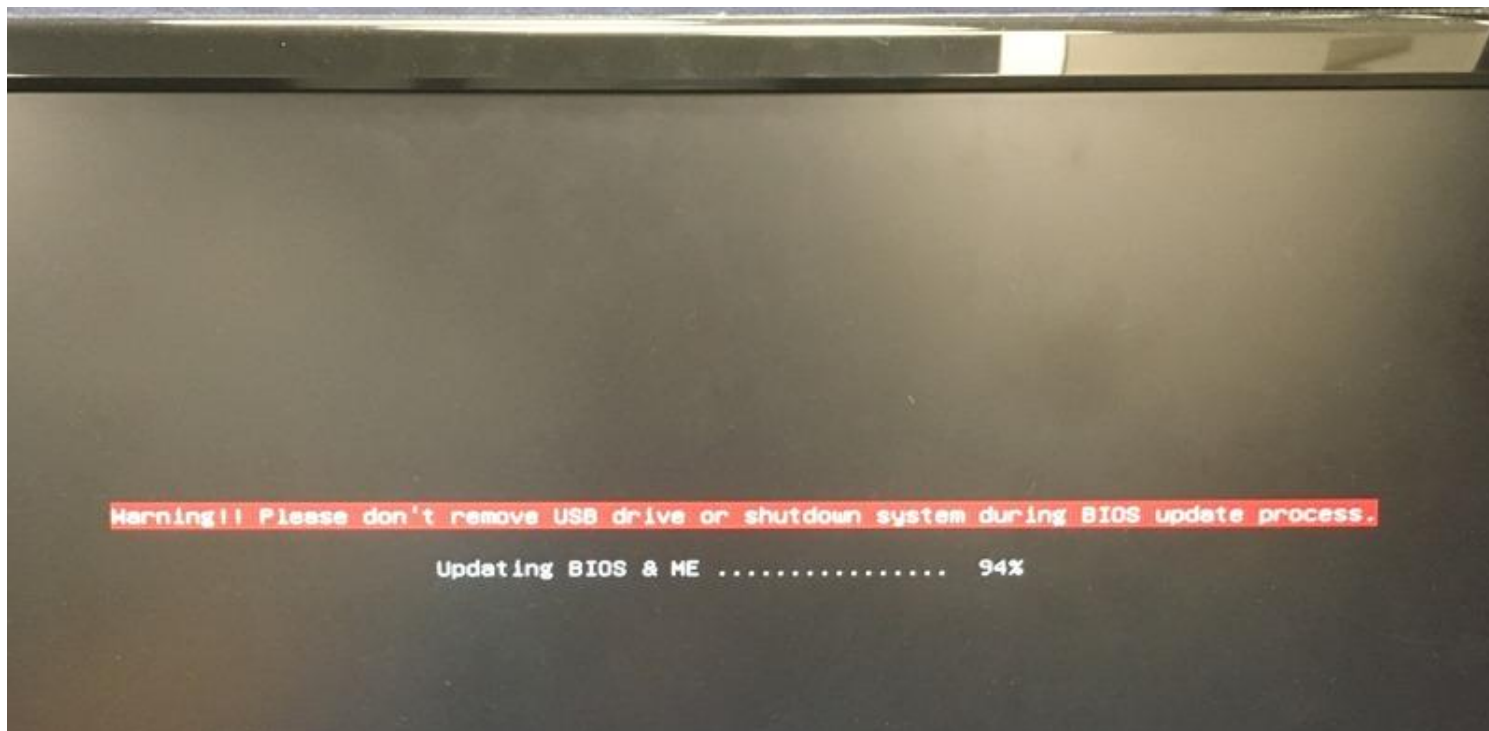
Step A-7 Flash BIOS by M-flash function

- It will be showed warning message - **System will be reset automatically to update BIOS after 5 seconds.**
- Note: **Don't remove USB driver or shutdown system.**



Step A-8 Flash BIOS by M-flash function

- It will be flashing BIOS and ME after reboot.



Step A-9 Flash BIOS by M-flash function

- Please into BIOS setup and the check BIOS version again.



Step B Use Intel-SA-00086 Detection Tool for checking.

- Please run Intel-SA-00086 Detection Tool for checking.
- It will be showed
“**This system is not vulnerable. It has already been patched.**”
or
“**This system is not vulnerable.**”
- Intel-SA-00086 Detection Tool is on Intel website as below link:
- <https://downloadcenter.intel.com/download/27150?v=t>

Risk Assessment

Based on the analysis performed by this tool: **This system is not vulnerable. It has already been patched.**

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: 1.0.0.152

Scan date: 1/9/2018 9:05:33 PM

Host Computer Information

Name: DESKTOP-V991IOB

Manufacturer: Micro-Star International Co., Ltd.

Model: H110 Gaming Trident 3 (MS-B906)

Processor Name: Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz

OS Version: Microsoft Windows 10 Home

Intel(R) ME Information

Engine: Intel(R) Management Engine

Version: 11.8.50.3399

SVN: 3



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: 1.0.0.152

Scan date: 1/10/2018 1:16:42 PM

Host Computer Information

Name: DESKTOP-ER3S5C7

Manufacturer: MICRO-STAR INTERNATIONAL CO., LTD

Model: MS-7887

Processor Name: Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz

OS Version: Microsoft Windows 10 Pro

Intel(R) ME Information

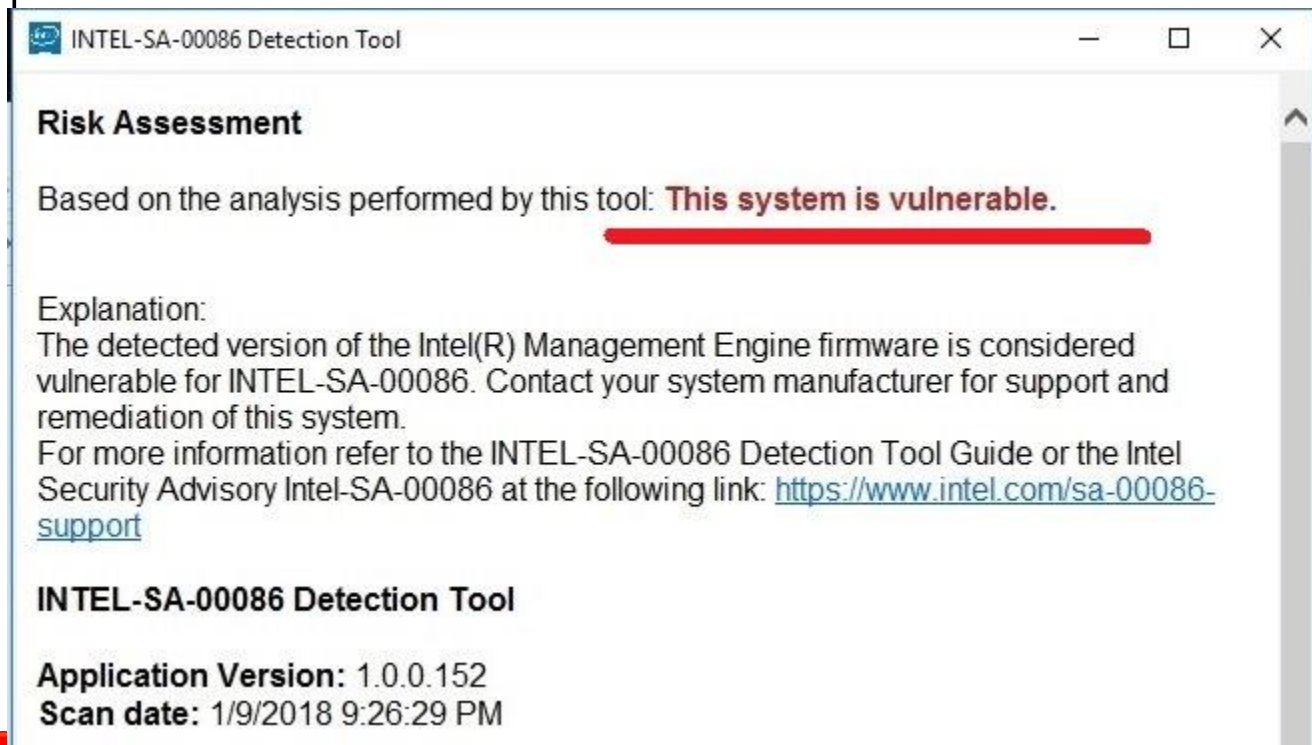
Engine: Intel(R) Management Engine

Version: 9.0.30.1482

SVN: 1

Before flash BIOS and update ME

- It will be showed “**This system is vulnerable.**” before flash BIOS and update ME.



Model list



- Cubi 3 Silent S / MS-B159 / BIOS version: EB159IMSV910
- Cubi 3 Silent / MS-B159 / BIOS version: EB159IMSV810
- Cubi 3 plus / MS-B164 / BIOS version: EB164IMSV812



msi[®]

TRUE  GAMING
SOME ARE PC, WE ARE GAMING