[How to] Protect Windows system against Intel Spectre and Meltdown Vulnerabilities (CVE 2017-5715, CVE-2018-3620, CVE-2018-3639, CVE-2018-3640, CVE-2018-3646)

MSI is aware of the discovered security vulnerabilities and have been working closely with Intel and Microsoft to address the issues, and will release the needed BIOS updates to reduce the risks.

How to mitigate these vulnerabilities?

- Update the latest processor microcode.
- Keep the operation system up to date at the latest build.
- Keep the anti-virus software up to date, and running at all times
- Make sure internet browser is always kept up to date with the latest updates and fixes
- Enable mitigations around Speculative Store Bypass (CVE-2018-3639)

Get the Processor Microcode Updates

[Method 1] Updating BIOS

For Intel SA-00115 & Intel SA-00161 vulnerabilities, MSI Notebooks with 8th & 7th Generation Intel CPU (Coffee Lake and Kaby Lake) would have microcode updated BIOS on the download webpage when they are available.

For Intel SA-00088 vulnerabilities, MSI Notebooks with 7th & 6th Generation Intel CPU (Kaby Lake and Sky Lake) have already updated the needed microcode, find the latest BIOS on the download webpage.

[Method 2] Get the stand-alone package from Windows Update

Go to Microsoft "Summary of Intel microcode updates" to get the latest Intel microcode updates which are related to Spectre Variant 3a (CVE-2018-3640: "Rogue System Register Read (RSRE)"), Spectre Variant 4 (CVE-2018-3639: "Speculative Store Bypass (SSB)"), and L1TF (CVE-2018-3620, CVE-2018-3646: "L1 Terminal Fault").

- KB4346084: Intel microcode updates for Window 10 RS4 1803
- KB4346085: Intel microcode updates for Window 10 RS3 1709

For Intel SA-00088 vulnerabilities, user can get this Intel microcode update via Windows Update automatically in Windows 10.

- KB4100347: Intel microcode updates for Window 10 RS4 1803

- KB4090007: Intel microcode updates for Window 10 RS3 1709

Get the OS Security Updates

Make sure to have the latest Windows 10 build (Windows 10 Version 1803, also known as April 2018 Update) updated by Knowledge Base 2410 and run Windows Update to get all patches released to against the attack.
Visit Microsoft page for further information.

Windows 10 Updates released to Intel vulnerabilities:
June 12, 2018—KB4284835 (OS Build 17134.112) for CVE-2018-3639
August 14, 2018—KB4343909 (OS Build 17134.228) for CVE-2018-3620 and CVE-2018-3646

*Microsoft Guidance:
Intel SA-00115 (CVE-2018-3639, CVE-2018-3640)
Intel SA-00161 (CVE-2018-3615, CVE-2018-3620, CVE-2018-3646)

Get the latest updates for anti-virus software, internet browsers and other application/programs.

Users who have the MSI pre-installed system, once the default Anti-Virus software is updated, the patch will be installed automatically after running Windows Update. For users who have installed their own system and run with other 3rd party Anti-Virus software, the Anti-Virus software might need an update in order to work with the latest Windows update. If you didn't receive the latest Windows Update, we suggest contacting the Anti-Virus software vendor for further assistance.

Some application/programs such as browsers or graphics driver might also be needed an update, we suggest to contact the device vendor or keep an eye on their sites to get the latest version updated.

More information for the CPU speculative execution side-channel vulnerabilities, please visit Intel websites.

Enable mitigations around Speculative Store Bypass (CVE-2018-3639)

Windows KB4284835 provides protections from an additional subclass of speculative execution side channel vulnerability known as Speculative Store Bypass (CVE-2018-3639).
These protections aren't enabled by default. For Windows client (IT pro) guidance, follow the instructions in KB4073119 and use this guidance document to enable mitigations for Speculative Store Bypass (CVE-2018-3639) in addition to the mitigations that have already been released for Spectre Variant 2 (CVE-2017-5715) and Meltdown (CVE-2017-5754).

*References:
Intel - Intel-SA-00115, Intel SA-00161, Intel Security Center
Microsoft - Microsoft Security Update Guide, Microcode Revision Guidance (*2018/08/08*), Get-SpeculationControlSettings PowerShell script, Protect your Windows devices against Spectre and Meltdown.