Getac's Statement on Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method

NOTICE: Getac is urgently working on qualifying and applying the fixes provided by Intel/ Microsoft on supported systems. Please continue to refer to Getac website to identify fixes as they are posted for your systems.

Release Date: Jan 10, 2018
Last Updated: Jan 10, 2018

Source: Intel / Microsoft

Summary:

Intel/Microsoft published Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

Details, please refer to Intel and Microsoft site.

Intel site: Speculative Execution and Indirect Branch Prediction Side Channel Analysis Method

Microsoft site: ADV180002 | Guidance to mitigate speculative execution side-channel vulnerabilities

Recommend:

1. Update the latest Microsoft KB or through January 2018 Windows security update.

   [Microsoft site: ADV180002 | Guidance to mitigate speculative execution side-channel vulnerabilities]

2. Update the latest BIOS w/ updated Microcode. Please check the affected products in table below:

IMPACTED PRODUCTS AND SOLUTION

Product name	CPU Generation	Current MCU version	ME MCU solution from intel	New BIOS version	Release Date	Latest BIOS Please download from Getac website
V110	4th Gen Core				2018/1/31	
	5th Gen Core				2018/1/31	
	6th Gen Core	0xBE	0xC2	R1.12.070520	2018/1/31	
F110	4th Gen Core	0x1C	0x21	R3.09.070520	2018/1/31	
	5th Gen Core	0x25	0x28	R1.16.070520	2018/1/31	
	6th Gen Core	0xBE	0xC2	R1.11.070520	2018/1/31	
	7th Gen Core	0x70	0x80		2018/1/31	
S410	6th Gen Core	0xBE	0xC2	R1.16.070520	2018/1/31	
	7th & 8th Gen Core	0x70	0x80		2018/1/31	
S400	~~3rd Gen Core~~	—	—		~~2018/1/31~~	
	4th Gen Core				2018/1/31	

B300	**4th Gen Core**				**2018/1/31**	
	6th Gen Core	**0xBE**	**0xC2**	**R1.12.070520**	**2018/1/31**	
A140	**6th Gen Core**	**0xBE**	**0xC2**	**R1.07.070520**	**2018/1/31**	
X500	**4th Gen Core**	**0x22**	**0x23**	**R3.16.070520**	**2018/1/31**	
	7th Gen Core	**0x70**	**0x80**		**2018/1/31**	
RX10	**5th Gen Core**	**0x25**	**0x28**	**R1.15.070520**	**Done**	**http://us.getac.com/support/drivers.html**
T800	**BYT-M**				**2018/1/31**	
	CHT T4				**2018/1/31**	
MX50	**CHT T3**				**2018/1/31**	
ZX70	**CHT T3**				**2018/1/31**	
EX80	**CHT T3**				**2018/1/31**	

Notes: the target plan of above schedule is subject to the testing status.

Related Information:

https://www.intel.com/content/www/us/en/support/articles/000025619/software.html

https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002

What are the associated CVEs for these vulnerabilities?

CVE-2017-5715

CVE-2017-5753

CVE-2017-5754