Product Notification

Document No. **Knowledge Base-A-1070112** **Revision** **1.0**

TOPIC:

Winmate update on Side Channel Analysis Security Issue

INTRODUCTION:

Winmate is aware of the new-side channel analysis vulnerabilities, known as Meltdown and Spectre, affecting many modern microprocessors that were discovered and published by a team of security researcher on January, 2018. A potential vulnerability in the x86 CPU architecture concerning a side channel analysis method. Malicious code using this method could infer data values from memory. The document highlights the resolution for the vulnerability.

RESOLUTIONS:

To mitigate the above-mentioned vulnerability, there are two essential components:

1. Intel is currently rolling out microcode updates for the CPU to address the hardware vulnerability, and these CPU microcode updates will be released by Winmate in the form of BIOS Update; Rollout schedule is dependent on Intel release progress.

   Important Notes:

   - The BIOS releases will be added or informed to customer(s) as the BIOS updates becomes available
   - Please contact our Sales Representative on how to receive the new BIOS update codes as they become available.

2. Microsoft also released OS updates (Windows 7 through Windows 10) to address the vulnerability. The update is currently available via Windows Update, and a standalone installable patch is also available from Microsoft. Below are the specific Windows Update references:

OS Security Update	Products
KB4056892	Windows 10, Windows Server 2016
KB4056891	Windows 10
KB4056890	Windows 10, Windows Server 2016
KB4056888	Windows 10
KB4056893	Windows 10 LTSB
KB4056898	Windows 8.1, Windows Server 2012 R2
KB4056897	Windows 7, Windows Embedded Standard 7, Windows server 2008 R2
KB4056894	Windows 7, Windows Embedded Standard 7, Windows server 2008 R2
KB4056895	Windows 8.1, Windows Server 2012 R2

Please go to Microsoft Security Advisory ADV180002 | Guidance to protect against the speculative execution side-channel vulnerabilities for further details

APPROVE: MD: EE: TE: PE:

WINMATE PRODUCTS AFFECTED:

Winmate's products with processors below are affected,

Intel® Processor	Code name
Intel® 3rd Generation Processor	Ivy Bridge
Intel® 4th Generation Processor	Haswell
Intel® 5th Generation Processor	Broadwell
Intel® 6th Generation Processor	Sky Lake
Intel® 7th Generation Processor	Kaby Lake
Intel® Atom® Processor	Cedar Trail
Intel® Atom® Processor	Valley View, platform Bay Trail
Intel® Atom® Processor	Cherry View, platform Braswell
Intel® Atom® Processor	Apollo Lake

References

Intel Security

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

RELEASE DATE:

January 12, 2018

ISSUED BY: **Michael Lee**

APPROVE: MD: EE: TE: PE: