Intel® Transactional Synchronization Extension (Intel® TSX) Disable Update for Selected Processors

Technical paper

June 2023

Revision 2.3

Document Number: 643557

Notice: This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Do not finalize a design with this information.

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document. The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Your costs and results may vary.

Contents

Revision History

Document Number	Revision Number	Description	Date
643557	1.5	New document number for NDA customers	November 2021
643557	2.0	Document repurposed to describe processors affected by Intel TSX defeaturing without PMU impact for IPU 2021.2	November 2021
643557	2.1	Added information for IA32_MCU_OPT_CTRL and Intel SGX	February 2022
643557	2.2	Updated Affected Processors.	February 2023
643557	2.3	Updated Affected Processors.	June 2023

1.0 Introduction

This whitepaper describes Intel® Transactional Synchronization Extension (Intel® TSX) behavior due to the updated microcode for 8th/10th generation Intel® Core™ processors, Intel® Pentium™ processors, and Intel® Celeron® processors based on the Whiskey Lake, Comet Lake, and Amber Lake microarchitectures, as well as 9th generation Intel® Core™ processors and Intel® Xeon® E processors based on Coffee Lake H microarchitecture.

In addition to the five CPUIDs that disable Intel TSX by default with the Intel Platform Update 2021.1 (IPU 2021.1) microcode (refer to the previous Performance Monitoring Impact of Intel® Transactional Synchronization Extensions Memory Ordering Issue White Paper (RDC 604224) for more information), Intel TSX will be disabled by default in two additional CPUIDs with IPU 2021.2. Workloads that benefited from Intel TSX might experience a change in performance. When the microcode released in IPU 2021.2 is applied, Intel TSX will be disabled by default on the processors described in the table below:

Table 1 Products affected by IPU 2021.2 microcode if Intel TSX is supported

Family-Model	Stepping	Processor Families / Processor Number Series
06_8EH	0xC	8th/10th generation Intel® Core™ processors, Intel® Pentium™ processors, and Intel® Celeron® processors based on Whiskey Lake, Comet Lake, and Amber Lake microarchitectures
06_9EH	0xD	9th generation Intel® Core™ processors and Intel® Xeon® E processors based on Coffee Lake H microarchitecture

The rest of this section describes the behavior of processors with these specific CPUIDs when the updated microcode is loaded.

A new CPUID bit, CPUID.07H.0H.EDX[11](RTM_ALWAYS_ABORT), will be enumerated, which is set to indicate to updated software that the loaded microcode is forcing Restricted Transactional Memory (RTM) abort. Information about the CPUID instruction is in the Processor Identification and Feature Determination section in the Intel Software Developer Manual.

In case the processor enumerated support for RTM previously, the CPUID enumeration bits for Intel TSX (CPUID.07H.0H.EBX[11] and CPUID.07H.0H.EBX[4]) continue to be set by default after the microcode update. Some workloads that benefited from Intel TSX might experience a change in performance.

On these processors, system software may use a bit in Model-Specific Register (MSR) 0x122, TSX_CTRL[TSX_CPUID_CLEAR], to clear the Hardware Lock Elision (HLE) and RTM CPUID bits to indicate to software that Intel TSX is disabled.

Table 2 IA32_TSX_CTRL MSR

Register address		Register Name / Bit fields	Bit Description	Comment
Hex	Dec			
122	290	IA32_TSX_CTRL		Thread scope. Not architecturally serializing. Available when CPUID.ARCH_CAP(EAX=7h,ECX=0):EDX[29] = 1 and IA32_ARCH_CAPABILITIES.bit 7 = 1
		0	RTM_DISABLE: When set to 1 XBEGIN will always abort with EAX code 0.	
		1	TSX_CPUID_CLEAR: When set to 1 CPUID.07h.EBX.RTM [bit 11] and CPUID.07h.EBX.HLE [bit 4] report 0. When set to 0 and the SKU supports TSX these bits will return 1.	

Although MSR 0x122 (TSX_CTRL) and MSR 0x123 (IA32_MCU_OPT_CTRL) can be used to re-enable Intel TSX for development, doing so is not recommended for production deployments. In particular, applying MD_CLEAR flows for mitigation of the Intel TSX Asynchronous Abort (TAA) transient execution attack may not be effective on these processors when Intel TSX is enabled with updated microcode. The processors continue to be mitigated against TAA when Intel TSX is disabled.

Note that if Intel® Software Guard Extensions (Intel® SGX) has been activated on the processor, it will not be possible to enable Intel TSX. In such cases, IA32_MCU_OPT_CTRL[RTM_LOCK] will read as 1.

Table 3 IA32_MCU_OPT_CTRL MSR

Register address		Register Name / Bit fields	Bit Description	Comment
Hex	Dec			
123	291	IA32_MCU_OPT_CTRL		Thread scope. Available when CPUID.(EAX=07H, ECX=0):EDX[9]=1
		1	RTM_ALLOW: When set to 0, XBEGIN will always abort with EAX code 0. When set to 1, XBEGIN behavior depends on the value of IA32_TSX_CTRL[RTM_DISABLE].	Read/Write. See below criteria for when RTM_ALLOW may be set.
		2	RTM_LOCKED: When 1, RTM_ALLOW is locked at zero, writes to RTM_ALLOW will be ignored	Read-Only status bit

Setting IA32_MCU_OPT_CTRL[RTM_ALLOW] to 1 is allowed if all the following criteria is met:

- IA32_ARCH_CAPABILITIES MSR is supported (CPUID.ARCH_CAP(EAX=07H,ECX=0):EDX[29] = 1)
- IA32_TSX_CTRL MSR is supported (IA32_ARCH_CAPABILITIES[TSX_CTRL] = 1)

- IA32_ARCH_CAPABILITIES[TAA_NO] = 0
- IA32_MCU_OPT_CTRL MSR is supported (CPUID.(EAX=07H,ECX=0):EDX[9]=1)
- IA32_MCU_OPT_CTRL[RTM_LOCKED] = 0

CPUID.07H.0H.EDX[11](RTM_ALWAYS_ABORT) = 1 or IA32_MCU_OPT_CTRL[RTM_ALLOW] = 1

§

2.0 MSR and Affected Processors for IPU 2021.1

This section summarizes the previously documented behavior for the five CPUIDs that disable Intel TSX by default with the Intel Platform Update 2021.1 (IPU 2021.1) microcode (refer to the previous Performance Monitoring Impact of Intel® Transactional Synchronization Extensions Memory Ordering Issue White Paper (PDF) for more information).

The updated definition of the thread-scope TSX_FORCE_ABORT MSR is described in the following table. Support of this updated MSR definition can be determined by checking for the combination of the following conditions:

CPUID.07H.0H.EDX[13](RTM_FORCE_ABORT) = 1

CPUID.07H.0H.EDX[11](RTM_ALWAYS_ABORT) = 1 or TSX_FORCE_ABORT[SDV_ENABLE_RTM] = 1

Although MSR 0x10F TSX_FORCE_ABORT is available to re-enable Intel TSX for development, it is not recommended for production. When RTM force abort is disabled in this way, RTM usage may be subject to memory-ordering correctness issues. Due to these issues, this unsupported mode should not be enabled for production use. System software might typically choose not to directly expose this functionality to users.

Table 4 Description of updated TSX_FORCE_ABORT_MSR

Register address		Register Name / Bit fields	Bit Description	Comment
Hex	Dec			
10f	271	TSX_FORCE_ABORT		
		0	RTM_FORCE_ABORT: Reads as 1, unless bit 2 is set. No implication on Counter 3.	Writes ignored, Default: 1
		1	TSX_CPUID_CLEAR: When set, CPUID.07H.0H.EBX[11]=0 and CPUID.07H.0H.EBX[4]=0.	R/W, Default: 0
		2	SDV_ENABLE_RTM: When set, processor may not force abort RTM. This unsupported mode should only be used for software development and not for production usage.	R/W, Default: 0
		3:63	Reserved	

Table 5 Affected products with Intel TSX disable microcode update

Family-Model	Stepping	Processor Families / Processor Number Series
06_4EH, 06_5EH	All	6th generation Intel® Core™ processors and Intel® Xeon® processor E3-1500m v5 product family and E3- 1200 v5 product family based on Skylake microarchitecture
06_8EH	<=0xB	7th/8th generation Intel® Core™ processors and Intel® Pentium™ processors based on Kaby Lake/Coffee Lake/Whiskey Lake microarchitecture
06_9EH	<=0xC	8th/9th generation Intel® Core™ processors and Intel® Pentium™ processors based on Coffee Lake microarchitecture

§