10th Generation Intel® Core™ Processor

Specification Update

Supporting 10th Generation Intel® Core™ Processor, Intel® Pentium® Processor, and Intel® Celeron® Processor for U/Y Processor Line Platforms, formerly known as Ice Lake

Revision 019

April 2024

Document Number: 341079-019

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis 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.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

All product plans and roadmaps are subject to change without notice.

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 technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

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.

Contents

Figures

Tables

Revision History

Revision Number	Description	Revision Date
001	• Initial release	August 2019
002	• Removed Errata ICL033 • Added Errata ICL034 to ICL044	November 2019
003	• Added Errata ICL045 to ICL057 • Added specification change 001 • Removed Erratum ICL037	May 2020
004	• Added Errata ICL058 to ICL069 • Updated Erratum ICL045 • Added specification change 002	August 2020
005	• Added Errata: ICL070, ICL071, ICL072	October 2020
006	• Added Erratum: ICL073 • Updated Erratum: ICL032	November 2020
007	• Updated Erratum: ICL024 • Fixed typo at Erratum ICL032 • Added Erratum: ICL074 • Removed Erratum: ICL074	January 2021
008	• Added Erratum: ICL075	February 2021
009	• Added Erratum: ICL076	March 2021
010	• Added Errata: ICL077, ICL078	April 2021
011	• Added Erratum: ICL079	June 2021
012	• Added Erratum: ICL080	August 2021
013	• Added Erratum: ICL081	October 2021
014	• Added Erratum: ICL082	March 2022
015	• Updated Erratum: ICL077	June 2022
016	• Added Errata: ICL083, ICL084	July 2022
017	• Added Erratum: ICL085	April 2023
018	• Added Erratum: ICL086	November 2023
019	• Added Erratum: ICL087	April 2024

§ §

Preface

This document is an update to the specifications contained in the documents listed in the following Affected Documents/Related Documents table. It is a compilation of device and document errata and specification clarifications and changes and is intended for hardware system manufacturers and for software developers of applications, operating system, and tools.

Information types defined in the Nomenclature section of this document are consolidated into this updated document and are no longer published in other documents. This document may also contain information that has not been previously published.

Affected Documents

Document Title	Document Number
10th Generation Intel® Core™ Processor Product Families Datasheet Volume 1 of 2	341077
10th Generation Intel® Core™ Processor Product Families Datasheet Volume 2 of 2	341078

Related Documents

Document Title	Document Number/Location
AP-485, Intel® Processor Identification and the CPUID Instruction	http://www.intel.com/design/processor/applnots/241618.htm
Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1: Basic Architecture Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A: Instruction Set Reference Manual A-M Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2B: Instruction Set Reference Manual N-Z Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A: System Programming Guide Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B: System Programming Guide Intel® 64 and IA-32 Intel® Architecture Optimization Reference Manual	http://www.intel.com/products/processor/manuals/index.htm
Intel® 64 and IA-32 Architectures Software Developer's Manual Documentation Changes	http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html

Document Title	Document Number/Location
Intel® Virtualization Technology Specification for Directed I/O Architecture Specification	D51397-001
ACPI Specifications	www.acpi.info

Nomenclature

Errata – These are design defects or errors. Errata may cause the processor's behavior to deviate from published specifications. Hardware and software designed to be used with any given stepping must assume that all errata documented for that stepping are present on all devices.

Specification Changes – These are modifications to the current published specifications. These changes will be incorporated in the next release of the specifications.

Specification Clarifications – This describe a specification in greater detail or further highlight a specification's impact to a complex design situation. These clarifications will be incorporated in the next release of the specifications.

Documentation Changes – This include typos, errors, or omissions from the current published specifications. These changes will be incorporated in the next release of the specifications.

Note: Errata remain in the specification update throughout the product's lifecycle, or until a particular stepping is no longer commercially available. Under these circumstances, errata removed from the specification update are archived and available upon request. Specification changes, specification clarifications, and documentation changes are removed from the specification update, when the appropriate changes are made to the appropriate product specification or user documentation (datasheets, manuals, etc.).

§ §

Identification Information

Component Identification via Programming Interface

The processor stepping can be identified by the following register contents:

Table 1. U/Y Processor Lines Component Identification

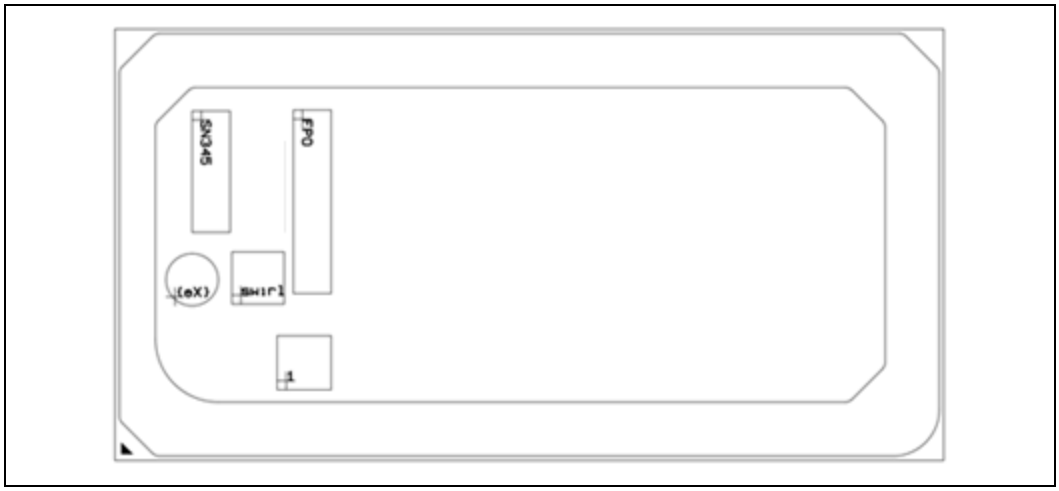
Samples	CPUID	Reserved [31:28]	Extended Family [27:20]	Extended Model [19:16]	Reserved [15:14]	Processor Type [13:12]	Family Code [11:8]	Model Number [7:4]	Stepping ID [3:0]
U	706E5h	Reserved	0000000b	0111b	Reserved	00b	0110b	1110b	0101b
Y	706E5h	Reserved	0000000b	0111b	Reserved	00b	0110b	1110b	0100b

1. The Extended Family, Bits [27:20] are used in conjunction with the Family Code, specified in Bits[11:8], to indicate whether the processor belongs to the Celeron™, Pentium™, or Intel® Core™ processor family.
2. The Extended Model, Bits [19:16] in conjunction with the Model Number, specified in Bits [7:4], are used to identify the model of the processor within the processor's family.
3. The Family Code corresponds to Bits [11:8] of the EDX register after RESET, Bits [11:8] of the EAX register after the CPUID instruction is executed with a 1 in the EAX register, and the generation field of the Device ID register accessible through Boundary Scan.
4. The Model Number corresponds to Bits [7:4] of the EDX register after RESET, Bits [7:4] of the EAX register after the CPUID instruction is executed with a 1 in the EAX register, and the model field of the Device ID register accessible through Boundary Scan.
5. The Stepping ID in Bits [3:0] indicates the revision number of that model. Refer Table 1 for the processor stepping ID number in the CPUID information.
6. When EAX is initialized to a value of '1', the CPUID instruction returns the Extended Family, Extended Model, Processor Type, Family Code, Model Number and Stepping ID value in the EAX register. The EDX processor signature value after reset is equivalent to the processor signature output value in the EAX register.

Cache and TLB descriptor parameters are provided in the EAX, EBX, ECX and EDX registers after the CPUID instruction is executed with a 2 in the EAX register.

Component Marking Information

Figure 1. Based on U-Processor Line Multi-Chip Package BGA Top-Side Markings



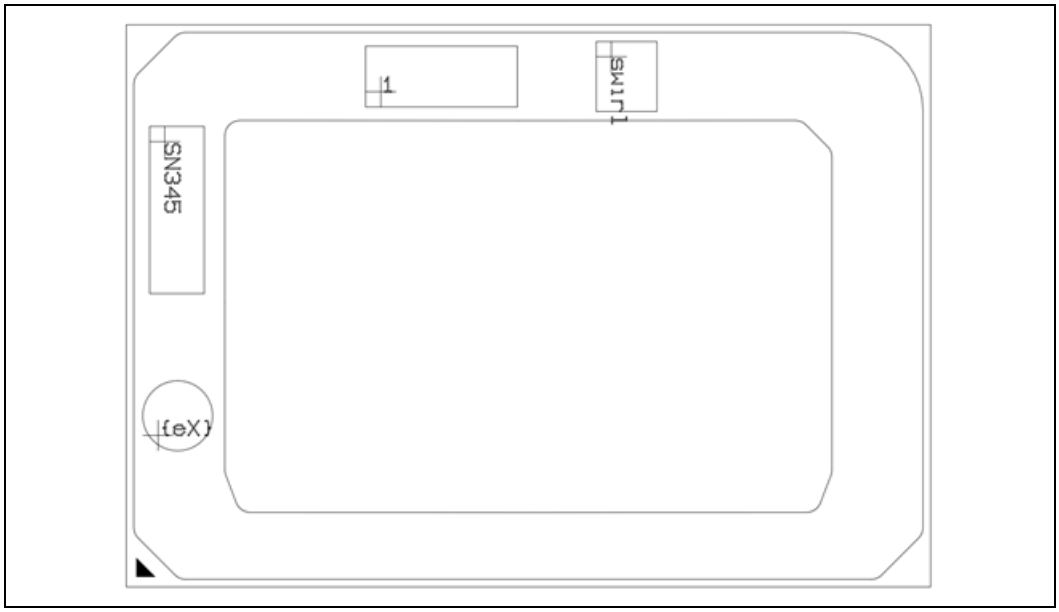
Pin Count: 1526 Package Size: 50 mm x 25 mm

Production (SSPEC):

- FPO: FPOxxxxx
- {eX}
- SWIR1: Intel® logo

Note: "1" is used to extract the unit visual ID (2D ID).

Figure 2. Based on Y-Processor Line Package BGA Top-Side Markings



Pin Count: 1377 Package Size: 26.5 mm x 18.5 mm

Production (SSPEC):
{eX}
SWIR1: Intel logo
Note: "1" is used to extract the unit visual ID (2D ID).

Note: Processor list can be found at:
https://ark.intel.com/content/www/us/en/ark/products/codename/74979/ice-lake.html

§§

Summary Tables of Changes

The following table indicates the Specification Changes, Errata, Specification Clarifications or Documentation Changes, which apply to the listed processor stepping. Intel intends to fix some of the errata in a future stepping of the component, and to account for the other outstanding issues through documentation or Specification Changes as noted. This table uses the following notations:

Codes Used in Summary Table

Stepping	Description
(No mark) or (Blank Box)	This erratum is fixed in listed stepping or specification change does not apply to listed stepping

Status	Description
Doc	Document change or update that will be implemented
Planned Fix	This erratum may be fixed in a future stepping of the product
Fixed	This erratum has been previously fixed in Intel® hardware, firmware, or software
No Fix	There are no plans to fix this erratum

Errata Summary Table

Erratum ID	Processor Line/ Stepping		Title
	U	Y	
ICL001	No Fix	No Fix	Incorrect Branch Predicted Bit in BTS/BTM Branch Records
ICL002	No Fix	No Fix	PEBS Eventing IP Field May be Incorrect After Not-Taken Branch
ICL003	No Fix	No Fix	Intel® PT TIP.PGD May not have Target IP Payload
ICL004	No Fix	No Fix	SMRAM State-Save Area Above the 4GB Boundary May Cause Unpredictable System Behavior
ICL005	No Fix	No Fix	x87 FPU Exception (#MF) May be Signaled Earlier than Expected
ICL006	No Fix	No Fix	Intel® Processor Trace PSB+ Packets May Contain Unexpected Packets
ICL007	No Fix	No Fix	Performance Monitoring Counters May Undercount When Using CPL Filtering
ICL008	No Fix	No Fix	Vector Masked Store Instructions May Cause Write Back of Cache Line Where Bytes are Masked

Erratum ID	Processor Line/ Stepping		Title
	U	Y	
ICL009	No Fix	No Fix	Incorrect FROM_IP Value for an RTM Abort in BTM or BTS May be Observed
ICL010	No Fix	No Fix	#GP on Segment Selector Descriptor that Straddles Canonical Boundary May Not Provide Correct Exception Error Code
ICL011	No Fix	No Fix	x87 FDP Value May be Saved Incorrectly
ICL012	No Fix	No Fix	Execution of VAESIMC or VAESKEYGENASSIST with an Illegal Value for VEX.vvvv May Produce a #NM Exception
ICL013	No Fix	No Fix	Execution of FXSAVE or FXRSTOR With the VEX Prefix May Produce a #NM Exception
ICL014	No Fix	No Fix	Writing Non-Zero Values to Read Only Fields in IA32_THERM_STATUS MSR May #GP
ICL015	No Fix	No Fix	Debug Exceptions May be Lost or Misreported When MOV SS or POP SS Instruction is Not Followed by a Write to SP
ICL016	No Fix	No Fix	Intel® PT VMentry Indication Depends on the Incorrect VMCS Control Field
ICL017	No Fix	No Fix	Execution of VAESENCLAST Instruction May Produce a #NM Exception Instead of a #UD Exception
ICL018	No Fix	No Fix	Performance Monitoring ASCI Status Bit May be Inaccurate
ICL019	No Fix	No Fix	Setting Performance Monitoring IA32_PERF_GLOBAL_STATUS_SET MSR Bit 63 May Not #GP
ICL020	No Fix	No Fix	WRMSR to PRMRR_MASK May Result in #GP When the Resulting PRMRR Range is Empty
ICL021	No Fix	No Fix	When Virtualization Exceptions are Enabled, EPT Violations May Generate Erroneous Virtualization Exceptions
ICL022	No Fix	No Fix	CPUID TLB Information is Inaccurate
ICL023	No Fix	No Fix	Performance Monitoring Load Latency Events May be Inaccurate for Gather Instructions
ICL024	No Fix	No Fix	CPUID L2 Cache Information May be Inaccurate
ICL025	No Fix	No Fix	Intel® SGX Enclave Accesses to the APIC-Access Page May Cause APIC-Access VM Exits
ICL026	No Fix	No Fix	Intel® PT PSB+ May be Lost
ICL027	No Fix	No Fix	Intel® PT CBR Packet May be Delayed or Silently Dropped
ICL028	No Fix	No Fix	Intel® PT TIP or FUP Packets May be Dropped Without OVF Packet
ICL029	No Fix	No Fix	Intel® PT Trace May Drop Second Byte of CYC Packet
ICL030	No Fix	No Fix	VM Entry That Clears TraceEn May Generate a FUP

Erratum ID	Processor Line/ Stepping		Title
	U	Y	
ICL031	No Fix	No Fix	VCVTPS2PH To Memory May Update MXCSR in the Case of a Fault on the Store
ICL032	No Fix	No Fix	PECI Frequency Limited to 3.2Kbps-1Mbps
ICL033	N/A		N/A. Erratum has been removed
ICL034	No Fix	No Fix	TCSS USB Host Controller (xHCI) May Hang
ICL035	Fixed	N/A	Unpopulated Type-C to Type-B or Type-A Converter (Cable or Dongle) May Degrade Type-C Port Functionality
ICL036	No Fix	No Fix	Swapping Devices on Type-C Ports in S3 May Degrade Type-C Port Functionality
ICL037	N/A	N/A	Duplicate of Erratum 039
ICL038	No Fix	No Fix	USB 3.1 Gen2 Link Compliance Test TD7.39 (Port Match Retry Test) May Fail
ICL039	Fixed	Fixed	The Processor May Consume Higher-Than-Expected Power During Light Workloads
ICL040	Fixed	Fixed	Processor May Hang When Both Threads are Active on a Physical Core
ICL041	Fixed	N/A	Processor May Hang During High-Throughput Graphics Scenarios
ICL042	Fixed	Fixed	PROCHOT De-assertion May Lead to False Processor LFM
ICL043	No Fix	No Fix	Some Errors Logged in IA32_MC1_STATUS May Not Generate Machine Check Exceptions
ICL044	Fixed	Fixed	The Processor May Assert THRMTRIP#
ICL045	No Fix	No Fix	Placing Page Table Information in the APIC-Access Page May Lead to Unexpected Page Faults While Performing Enclave Accesses
ICL046	No Fix	No Fix	Instruction Fetch May Cause Machine Check if Page Size Was Changed Without Invalidation
ICL047	Fixed	Fixed	System May Hang When Graphics Core is Running in Low Frequency Mode
ICL048	Fixed	Fixed	USB 3.x Devices May Not Enumerate or May Downgrade to USB2 Speeds on Ports Without a Retimer
ICL049	Fixed	Fixed	Isochronous Devices May Experience Deferred Memory Accesses
ICL050	Fixed	Fixed	FIVR PS5 Insufficient Current During PKG-C6 Resume
ICL051	Fixed	Fixed	LPDDR4x May Incorrectly Exit Self-Refresh
ICL052	Fixed	N/A	Incorrect TCSS DTS When a Thunderbolt™ Device is Connected

Erratum ID	Processor Line/ Stepping		Title
	U	Y	
ICL053	Fixed	Fixed	REP MOVSB Instruction to or From A Non-flat Segment May Cause Unpredictable System Behavior
ICL054	No Fix	No Fix	MASKMOV* Instruction to a Physical Memory Location Mapped by Two Linear Addresses of Different Page Sizes May Result in Unpredictable System Behavior
ICL055	Fixed	Fixed	USB 3.x Link Training Failure
ICL056	Fixed	Fixed	VTd DMA Remapping Disable in Gfx IOMMU May Cause Display Artifacts or Flickering
ICL057	Fixed	Fixed	MDS_NO Bit in IA32_ARCH_CAPABILITIES MSR is Incorrectly Set
ICL058	No Fix	No Fix	Overflow Flag in IA32_MC0_STATUS MSR May be Incorrectly Set
ICL059	No Fix	No Fix	IA32_L3_QOS_Mask_N Accepts Non-Contiguous Masks
ICL060	No Fix	No Fix	System May Hang When CR0.TS Or CR0.EM are Set
ICL061	Fixed	Fixed	Processor May Experience Unexpected System Behaviour When CR0.TS Or CR0.EM are Set
ICL062	No Fix	No Fix	Wrong Page Access Semantics May be Reported When Intel® SGX ENCLU[EMODPE] Instruction Generates Page Fault (#PF) Exception
ICL063	Fixed	Fixed	Usage of Bit 55 of IA32_TSC_DEADLINE MSR May Cause Spurious Timer Interrupt
ICL064	Fixed	Fixed	Time Stamp Counters May Contain A Shifted Time Value
ICL065	Fixed	Fixed	Unpredictable System Behaviour Due to Move Elimination
ICL066	Fixed	Fixed	REP MOVSB Might Lead to Incorrect ESP
ICL067	Fixed	Fixed	A Ring Interconnect Performance State Transition May Result in Unpredictable System Behaviour
ICL068	No Fix	No Fix	Uncore Performance Monitoring Controls May Not Function Properly
ICL069	Fixed	Fixed	A Memory Controller Domain Low Power Mode Transition May Result in Retrieval of Incorrect Data from Memory
ICL070	Fixed	Fixed	VT-d Domain-Specific Context Cache Invalidation Requests May Not Complete
ICL071	Fixed	Fixed	Type-C Ports Configured as DP-FIXD May Lead to System Hang
ICL072	No Fix	No Fix	VERR Instruction Inside VM-entry May Cause DR6 to Contain Incorrect Values
ICL073	No Fix	No Fix	Processor May Hang if Warm Reset Triggers During BIOS Initialization
ICL074	N/A	N/A	N/A. Erratum has been Removed.

Erratum ID	Processor Line/ Stepping		Title
	U	Y	
ICL075	No Fix	No Fix	IA32_RTIT_STATUS.FilterEn Bit Might Reflect A Previous Value
ICL076	Fixed	Fixed	SSBD May Not Properly Restrict Load Execution
ICL077	No Fix	No Fix	Executing an XSAVE or VZEROALL Instruction After SYSENTER May Result in Unexpected SSE/AVX Register Values
ICL078	No Fix	No Fix	False MC1 Error Reported in the Shadow of an Internal Timer Error
ICL079	No Fix	No Fix	Placing Posted-Interrupt Descriptors Within the PRMRR May Result in a Processor Hang
ICL080	No Fix	No Fix	System May Experience an Internal Timeout Error When Directing Intel® PT to a Small, Uncacheable, Single-Range Output Buffer
ICL081	No Fix	No Fix	Setting MISC_FEATURE_CONTROL.DISABLE_THREE_STRIKE_CNT Does Not Prevent the Three-strike Counter from Incrementing
ICL082	No Fix	No Fix	Intel® PT Trace May Contain Incorrect Data When Configured with Single Range Output Larger Than 4KB
ICL083	No Fix	No Fix	Incorrect MCACOD For L2 Prefetch MCE
ICL084	No Fix	No Fix	Call Instruction Wrapping Around The 32-bit Address Boundary May Return to Incorrect Address
ICL085	Fixed	Fixed	Branch Predictor May Produce Incorrect Instruction Pointer
ICL086	No Fix	No Fix	USB 3.2 DbC Sublink Speed Attribute ID (SSID) Value
ICL087	No Fix	No Fix	A Write to The TSC_Deadline MSR May Cause an Unexpected Timer Interrupt

Specification Changes

No.	Specification Changes
001	PKG-C9 disabled
002	FIVR Power state 5 (PS5) disabled

Specification Clarifications

No.	Specification Clarifications
	None for this revision of this specification update.

Documentation Changes

No.	Documentation Changes
	None for this revision of this specification update.

§ §

Errata Details

ICL001	Incorrect Branch Predicted Bit in BTS/BTM Branch Records
Problem	Branch Trace Store (BTS) and Branch Trace Message (BTM) send branch records to the Debug Store management area and system bus respectively. The Branch Predicted bit (bit 4 of eighth byte in BTS/BTM records) should report whether the most recent branch was predicted correctly. Due to this erratum, the Branch Predicted bit may be incorrect.
Implication	BTS and BTM cannot be used to determine the accuracy of branch prediction.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL002	PEBS Eventing IP Field May be Incorrect after Not-Taken Branch
Problem	When a Precise-Event-Based-Sampling (PEBS) record is logged immediately after a not-taken conditional branch (Jcc instruction), the Eventing IP field should contain the address of the first byte of the Jcc instruction. Due to this erratum, it may instead contain the address of the instruction preceding the Jcc instruction.
Implication	Performance monitoring software using PEBS may incorrectly attribute PEBS events that occur on a Jcc to the preceding instruction.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL003	Intel® PT TIP.PGD May Not Have Target IP Payload
Problem	When Intel® Processor Trace (Intel® PT) is enabled and a direct unconditional branch clears IA32_RTIT_STATUS.FilterEn (MSR 571H, bit 0), due to this erratum, the resulting Target IP Packet, Packet Generation Disable (TIP.PGD) may not have an IP payload with the target IP.
Implication	It may not be possible to tell which instruction in the flow caused the TIP.PGD using only the information in trace packets when this erratum occurs.
Workaround	The Intel® Processor Trace decoder can compare direct unconditional branch targets in the source with the FilterEn address range(s) to determine which branch cleared FilterEn.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL004	SMRAM State-Save Area above the 4GB Boundary May Cause Unpredictable System Behavior
Problem	If BIOS uses the RSM instruction to load the SMBASE register with a value that would cause any part of the SMRAM state-save area to have an address above 4-GBytes, subsequent transitions into and out of SMM (System-Management Mode) might save and restore processor state from incorrect addresses.
Implication	This erratum may cause unpredictable system behavior. Intel has not observed this erratum with any commercially available system.

Workaround	Ensure that the SMRAM state-save area is located entirely below the 4GB address boundary.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL005	**x87 FPU Exception (#MF) May be Signaled Earlier than Expected**
Problem	x87 instructions that trigger #MF normally service interrupts before the #MF. Due to this erratum, if an instruction that triggers #MF is executing when an Enhanced Intel SpeedStep® Technology transitions, an Intel® Turbo Boost Technology transitions, or a Thermal Monitor event occurs, the #MF may be taken before pending interrupts are serviced.
Implication	Software may observe #MF being signaled before pending interrupts are serviced.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL006	**Intel® Processor Trace PSB + Packets May Contain Unexpected Packets**
Problem	Some Intel® Processor Trace packets should be issued only between Target IP Packet.Packet Generation Enable (TIP.PGE) and Target IP Packet. Generation Disable (TIP.PGD) packets. Due to this erratum, when a TIP.PGE packet is generated, it may be preceded by a Packet Stream Boundary (PSB) that incorrectly includes Flow Update Packet (FUP) and MODE.Exec packets.
Implication	Due to this erratum, FUP and MODE.Exec may be generated unexpectedly.
Workaround	Decoders should ignore FUP and MODE.Exec packets that are not between TIP.PGE and TIP.PGD packets.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL007	**Performance Monitoring Counters May Undercount When Using CPL Filtering**
Problem	Performance Monitoring counters configured to count only OS or only USR events by setting exactly one of bits 16 or 17 in IA32_PERFEVTSELx MSRs (186H-18DH) may not count for a brief period during the transition to a new CPL.
Implication	A measurement of ring transitions (using the edge-detect bit 18 in IA32_PERFEVTSELx) may undercount, such as CPL_CYCLES.RING0_TRANS (Event 5CH, Umask 01H). Additionally, the sum of an OS-only event and a USR-only event may not exactly equal an event counting both OS and USR. Intel has not observed any other software-visible impact
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL008	**Vector Masked Store Instructions May Cause Write Back of Cache Line Where Bytes Are Masked**
Problem	Vector masked store instructions to WB (write-back) memory-type that cross cache lines may lead to CPU writing back cached data even for cache lines where all of the bytes are masked. This can affect MMIO (Memory Mapped IO) or non-coherent agents in the following ways: • For MMIO range that is mapped as WB memory type, this erratum may lead to Machine Check Exception (MCE) due to writing back data into the MMIO space. This applies only to cross page vector masked stores where one of the pages is in MMIO range.

	• If the CPU cached data is stale, for example in the case of memory written directly by a non-coherent agent (agent that uses non-coherent writes), this erratum may lead to writing back stale cached data even if these bytes are masked.
Implication	CPU may generate writes into MMIO space which lead to MCE or may write stale data into memory also written by non-coherent agents.
Workaround	It is recommended not to map MMIO range as WB. If WB is used for MMIO range, OS or VMM should not map such MMIO page adjacent to a regular WB page (adjacent on the linear address space, before or after the IO page). Memory that may be written by non-coherent agents should be separated by at least 64 bytes from regular memory used for other purposes (on the linear address space).
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL009	**Incorrect FROM_IP Value for an RTM Abort in BTM or BTS May be Observed**
Problem	During Restricted Transactional Memory (RTM) operation when branch tracing is enabled using Branch Trace Message (BTM) or Branch Trace Store (BTS), the incorrect EIP value (From_IP pointer) may be observed for an RTM abort.
Implication	Due to this erratum, the From_IP pointer may be the same as that of the immediately preceding taken branch.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL010	**#GP on Segment Selector Descriptor that Straddles Canonical Boundary May Not Provide Correct Exception Error Code**
Problem	During a # General Protection Exception (GPE), the processor pushes an error code on to the exception handler's stack. If the segment selector descriptor straddles the canonical boundary, the error code pushed onto the stack may be incorrect.
Implication	An incorrect error code may be pushed onto the stack. Intel has not observed this erratum with any commercially available software.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL011	**x87 FDP Value May be Saved Incorrectly**
Problem	Execution of the FSAVE, FNSAVE, FSTENV, or FNSTENV instructions in real-address mode or virtual-8086 mode may save an incorrect value for the x87 FPU data pointer (FDP). This erratum does not apply if the last non-control x87 instruction had an unmasked exception.
Implication	Software operating in real-address mode or virtual-8086 mode that depends on the FDP value for non-control x87 instructions without unmasked exceptions may not operate properly.
Workaround	None identified. Software should use the FDP value saved by the listed instructions only when the most recent non-control x87 instruction incurred an unmasked exception.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL012	Execution of VAESIMC or VAESKEYGENASSIST With an Illegal Value for VEX.vvvv May Produce a #NM Exception
Problem	The VAESIMC and VAESKEYGENASSIST instructions should produce a #UD (Invalid-Opcode) exception if the value of the vvvv field in the VEX prefix is not 1111b. Due to this erratum, if CR0.TS is "1", the processor may instead produce a #NM (Device-Not-Available) exception.
Implication	Due to this erratum, some undefined instruction encodings may produce a #NM instead of a #UD exception.
Workaround	Software should always set the vvvv field of the VEX prefix to 1111b for instances of the VAESIMC and VAESKEYGENASSIST instructions.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL013	Execution of FXSAVE or FXRSTOR With the VEX Prefix May Produce a #NM Exception
Problem	Attempt to use FXSAVE or FXRSTOR with a VEX prefix should produce a #UD (Invalid-Opcode) exception. If either the TS or EM flag bits in CR0 are set, a #NM (device-not-available) exception will be raised instead of #UD exception.
Implication	Due to this erratum a #NM exception may be signaled instead of a #UD exception on an FXSAVE or an FXRSTOR with a VEX prefix.
Workaround	Software should not use FXSAVE or FXRSTOR with the VEX prefix.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL014	Writing Non-Zero Values to Read Only Fields in IA32_THERM_STATUS MSR May #GP
Problem	IA32_THERM_STATUS MSR (19CH) includes read-only (RO) fields as well as writable fields. Writing a non-zero value to any of the read-only fields may cause a #GP.
Implication	Due to this erratum, software that reads the IA32_THERM_STATUS MSR, modifies some of the writable fields, and attempts to write the MSR back may #GP.
Workaround	Software should clear all read-only fields before writing to this MSR.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL015	Debug Exceptions May be Lost or Misreported When MOV SS or POP SS Instruction is Not Followed by a Write to SP
Problem	If a MOV SS or POP SS instruction generated a debug exception and is not followed by an explicit write to the stack pointer (SP), the processor may fail to deliver the debug exception or, if it does, the DR6 register contents may not correctly reflect the causes of the debug exception.
Implication	Debugging software may fail to operate properly if a debug exception is lost or does not report complete information. Intel has not observed this erratum with any commercially available software.
Workaround	Software should explicitly write to the stack pointer immediately after executing MOV SS or POP SS.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL016	Intel® PT VMentry Indication Depends on the Incorrect VMCS Control Field
Problem	An Intel® Processor Trace PIP (Paging Information Packet), which includes indication of entry into non-root operation, will be generated on VMentry as long as the "Conceal VMX in Intel® PT" field (bit 19) in Secondary Execution Control register (IA32_VMX_PROCBASED_CTLS2, MSR 048BH) is clear. This diverges from expected behavior, since this PIP should instead be generated only with a zero value of the "Conceal VMX entries from Intel® PT" field (Bit 17) in the Entry Control register (IA32_VMX_ENTRY_CTLS MSR 0484H).
Implication	An Intel® PT trace may incorrectly expose entry to non-root operation.
Workaround	A VMM (Virtual Machine Monitor) should always set both the "Conceal VMX entries from Intel® PT" field in the Entry Control register and the "Conceal VMX in Intel® PT" in the Secondary Execution Control register to the same value.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL017	Execution of VAESENCLAST Instruction May Produce a #NM Exception Instead of a #UD Exception
Problem	Execution of VAESENCLAST with VEX.L= 1 should signal a #UD (Invalid Opcode) exception, however, due to the erratum, a #NM (Device Not Available) exception may be signaled.
Implication	As a result of this erratum, an operating system may restore AVX and other state unnecessarily.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL018	Performance Monitoring ASCI Status Bit May be Inaccurate
Problem	The Anti Side-Channel Interference (ASCI) field in IA32_PERF_GLOBAL_STATUS (MSR 38EH, bit 60) should be set when the count in any of the configured performance counters (Example: IA32_PMCx or IA32_FIXED_CTRx) was altered due to direct or indirect operation of Intel® SGX. Due to this erratum, the ASCI bit may not be set properly when IA32_FIXED_CTR0 is used.
Implication	Software that relies on the value of the ASCI bit in IA32_PERF_GLOBAL_STATUS for its operation may not operate correctly when IA32_FIXED_CTR0 is used.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL019	Setting Performance Monitoring IA32_PERF_GLOBAL_STATUS_SET MSR Bit 63 May Not #GP
Problem	Bit 63 of IA32_PERF_GLOBAL_STATUS_SET MSR (391H) is reserved. Due to this erratum, setting the bit will not result in General Protection Fault (#GP).
Implication	Software that attempts to set bit 63 of IA32_PERF_GLOBAL_STATUS_SET MSR does not generate #GP. There are no other system implications to this behavior.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL020	WRMSR to PRMRR_MASK May Result in #GP When the Resulting PRMRR Range is Empty
Problem	WRMSR to PRMRR_MASK (MSR 1F5H) may result in a #GP (General Protection Fault) when the resulting PRMRR (Processor Reserved Memory Range Register) base (as defined by MSR 1F4H) bitwise-and with its mask (as defined by MSR 1F5) equals zero, the range is configured (bit 3 of MSR 1F4H), and the processor is running with Intel Hyper Threading (HT) technology disabled.
Implication	WRMSR to PRMRR_MASK may result in a #GP. Intel has not observed this erratum with any commercially available software.
Workaround	Software should not configure an empty PRMRR range.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL021	When Virtualization Exceptions are Enabled, EPT Violations May Generate Erroneous Virtualization Exceptions
Problem	An access to a GPA (guest-physical address) may cause an EPT-violation VM exit. When the "EPT-violation #VE" VM-execution control is 1, an EPT violation may cause a #VE (virtualization exception) instead of a VM exit. Due to this erratum, an EPT violation may erroneously cause a #VE when the "suppress #VE" bit is set in the EPT paging-structure entry used to map the GPA being accessed. This erratum does not apply when the "EPT-violation #VE" VM-execution control is 0 or when delivering an event through the IDT. This erratum applies only when the GPA in CR3 is used to access the root of the guest paging-structure hierarchy (or, with PAE paging, when the GPA in a PDPTE is used to access a page directory).
Implication	When using PAE paging mode, an EPT violation that should cause an VMexit in the VMM may instead cause a VE# in the guest. In other paging modes, in addition to delivery of the erroneous #VE, the #VE may itself cause an EPT violation, but this EPT violation will be correctly delivered to the VMM.
Workaround	A VMM may support an interface that guest software can invoke with the VMCALL instruction when it detects an erroneous #VE.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL022	CPUID TLB Information is Inaccurate
Problem	CPUID leaf 16 (EAX=16H) subleaf 1 (ECX=01H) TLB information inaccurately reports that the instructions' 1st-level TLB is 8-way and supports both 4K and 2M/4M pages, although it is split into 16 sets of 8 ways for 4K pages and 2 sets of 8 ways for 2M/4M pages.
Implication	Software that uses CPUID instructions 1st-level TLB information may operate incorrectly. Intel has not observed this erratum to impact the operation of any commercially available software.
Workaround	None identified. Software should ignore instructions' 1st-level TLB information reported by CPUID for the affected processors.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL023	Performance Monitoring Load Latency Events May be Inaccurate for Gather Instructions
Problem	The performance monitoring events MEM_TRANS_RETIRED.LOAD_LATENCY_* (Event CDH; UMask 01H; any latency) count load instructions whose latency exceed a predefined threshold, where the loads are randomly selected using the load latency facility (an extension of PEBS). However due to this erratum, these events may count incorrectly for VGATHER*/VPGATHER* instructions.
Implication	The Load Latency Performance Monitoring events may be Inaccurate for Gather instructions.
Workaround	None identified
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL024	CPUID L2 Cache Information May be Inaccurate
Problem	CPUID extended function 80000006H (EAX=80000006H) inaccurately reports information about the L2 cache in ECX. The function reports that the L2 cache size is 256K divided into 8 ways, while the actual L2 size and structure should be inferred from reading CPUID leaf 04H sub-leaf 02H.
Implication	Software that uses CPUID extended leaf 80000006H L2 cache information may operate incorrectly. Intel has not observed this erratum to impact the operation of any commercially available software.
Workaround	None identified. Software should ignore the L2 cache size information reported by CPUID extended leaf 80000006H for the affected processors.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL025	Intel® SGX Enclave Accesses to the APIC-Access Page May Cause APIC-Access VM Exits
Problem	In VMX non-root operation, Intel® Software Guard Extensions (Intel® SGX) enclave accesses to the APIC-access page may cause APIC-access VM exits instead of page faults.
Implication	A virtual-machine monitor (VMM) may receive a VM exit due to an access that should have caused a page fault, which would be handled by the guest operating system (OS).
Workaround	A VMM avoids this erratum if it does not map any part of the Enclave Page Cache (EPC) to the guest's APIC-access address; an operating system avoids this erratum if it does not attempt indirect enclave accesses to the APIC.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL026	Intel® PT PSB + May Be Lost
Problem	Intel® PT (Intel® Processor Trace) generates a PSB+ (Packet Stream Boundary+) set of packets periodically, based on the number of trace bytes written out. If the threshold for a PSB+ is reached while Intel® PT is being disabled by clearing IA32_RTIT_CTL.TraceEn[0] (MSR 0570H) either during a VM-exit or after generating fewer than 8 bytes of trace since TraceEn was last set, that PSB+ may be lost.
Implication	An Intel® PT decoder that is scanning for a PSB+ at which to begin decoding may have to skip over more trace output bytes before finding one.

Workaround	Software processing the trace at runtime can detect that a PSB+ was dropped by checking that IA32_RTIT_STATUS.PacketByteCnt[48:32] (MSR 0571H) has recently crossed the PSB threshold, while scanning the trace to check that the expected PSB+ was not inserted. When a dropped PSB+ is detected, software can force a PSB+ to be inserted the next time Intel® PT is enabled by clearing PacketByteCnt.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL027	**Intel® PT CBR Packet May be Delayed or Dropped**
Problem	Due to a complex set of microarchitectural conditions, the Intel® PT (Intel® Processor Trace) CBR (Core:Bus Ratio) packet generated on a frequency change may be dropped, without an OVF (Overflow) packet, or may be inserted into the trace late, after other packets (including possibly another CBR) that were generated after the frequency change completed.
Implication	An Intel® PT decoder may report an incorrect core: bus ratio to a portion of the trace, which may result in an incorrect wall clock time calculation.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL028	**Intel® PT TIP or FUP Packets May be Dropped without OVF Packet**
Problem	The Intel® PT (Intel® Processor Trace) OVF (Overflow) packet may not be generated when only TIPs (Target IP Packets) and/or FUPs (Flow Update Packets) are lost due to internal buffer overflow.
Implication	A decoder error will result from the missing FUP and/or TIP packets.
Workaround	None identified. An Intel® PT decoder will be able to resume proper decode from the next FUP, TIP, or PSB (Packet Stream Boundary) packet. The incidence of error may be mitigated by setting IA32_RTIT_CTL.CYCEn[bit 1] (MSR 0570H) to 1, as an internal buffer overflow that loses a CYC packet will generate an OVF.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL029	**Intel® PT Trace May Drop Second Byte of CYC Packet**
Problem	Due to a rare microarchitectural condition, the second byte of a 2-byte CYC (Cycle Count) packet may be dropped without an OVF (Overflow) packet.
Implication	A trace decoder may signal a decode error due to the lost trace byte.
Workaround	None Identified. A mitigation is available for this erratum. If a decoder encounters a multi-byte CYC packet where the second byte has bit 0 (Ext) set to 1, it should assume that 4095 cycles have passed since the prior CYC packet, and it should ignore the first byte of the CYC and treat the second byte as the start of a new packet.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL030	**VM Entry that Clears TraceEn May Generate A FUP**
Problem	If VM entry clears Intel® Processor Trace (Intel® PT) IA32_RTIT_CTL.TraceEn (MSR 570H, bit 0) while PacketEn is 1 then a Flow Update Packet (FUP) will precede the Target IP Packet, Packet Generation Disable (TIP.PGD). VM entry can clear TraceEn if the VM-entry MSR-load area includes an entry for the IA32_RTIT_CTL MSR.

ICL030	VM Entry that Clears TraceEn May Generate A FUP
Implication	When this erratum occurs, an unexpected FUP may be generated that creates the appearance of an asynchronous event take place immediately before or during the VM entry.
Workaround	The Intel® PT trace decoder may opt to ignore any FUP whose IP matches that of a VM entry instruction.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL031	VCVTPS2PH To Memory May Update MXCSR in the Case of a Fault on the Store
Problem	Execution of the VCVTPS2PH instruction with a memory destination may update the MXCSR exceptions flags (bits [5:0]) if the store to memory causes a fault (Example: #PF) or VM exit. The value written to the MXCSR exceptions flags is what would have been written if there were no fault.
Implication	Software may see exceptions flags set in MXCSR, although the instruction has not successfully completed due to a fault on the memory operation. Intel has not observed this erratum to affect any commercially available software.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL032	PECI Frequency Limited to 3.2Kbps-1Mbps
Problem	The PECI (Platform Environmental Control Interface) 3.1 specification's operating frequency range is 2Kbps to 2Mbps. Due to this erratum, PECI may be unreliable when operated out of 3.2Kbps-1Mbps range.
Implication	Platforms attempting to run PECI out of 3.2Kbps-1Mbps range may not behave as expected.
Workaround	None identified. Platforms should limit PECI operating frequency to 3.2Kbps-1Mbps range.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL033	N/A. Erratum has been Removed

ICL034	TCSS USB Host Controller (xHCI) May Hang
Problem	TCSS USB Host Controller (xHCI) may hang when a USB 3.x Device requests U2 exit and the xHCI controller is entering autonomous power gated state (d0i2) asynchronous occur at the same time.
Implication	Due to this erratum, the system may hang.
Workaround	A workaround has been implemented in IOM Firmware 04.00C.0.00 and later disabling d0i2. System power implications are USB3.x device and workload dependent.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL035	Unpopulated Type C to Type B or Type A Converter (Cable or Dongle) May Degrade Type C Port Functionality
Problem	Connecting a USB Device to Type-C Converter cable or a dongle to Type-B or Type-A Connector on an unpopulated Type-C port may align with Processor Power Management (PM) transition causing a momentary stall of the Processor PM Transition. This may result in the violation of a Device reported Latency Tolerance Reporting (LTR).
Implication	Isochronous traffic streams may exhibit temporary anomalies when this erratum occurs, such as audio clicks or display flickers.
Workaround	A Fix has been implemented in IOM Firmware 04.00F.0.00
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL036	Swapping Devices on Type C Ports in S3 May Degrade Type C Port Functionality
Problem	If a USB 3.x device is established to operate in USB 2.0 and the platform enters an S3 state, if a different USB 3.x device is connected to the port, the speed will be limited to USB 2.0 speed operation.
Implication	Due to this erratum, the USB 3.x device may only operate at USB 2.0 speeds.
Workaround	None identified. USB 3.x capability can be recovered by unplugging and re-plugging the USB 3.x device after the system has resumed from S3.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL037	N/A. Erratum has been Removed.

ICL038	USB 3.1 Gen2 Link Compliance Test TD7.39 (Port Match Retry Test) May Fail
Problem	While running USB 3.1 Gen2 Link Compliance Test TD7.39 (Port Match Retry Test), the speed negotiation may downgrade to USB 2.0 instead of USB 3.1 Gen1 when using an USB cable not capable of USB 3.1 Gen2 speeds.
Implication	USB 3.1 Gen2 link may downgrade to USB 2.0 when using an USB cable to capable of USB 3.1 Gen2 speeds and fail the certification test.
Workaround	None identified. Intel has obtained a waiver for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL039	The Processor May Consume Higher-Than-Expected Power During Light Workloads
Problem	The processor's internal voltage regulation circuits optimize power consumption based on processor workload. Due to this erratum, these circuits may fail to completely optimize power under certain lightly loaded conditions when TCSS is in TC Cold state.
Implication	When this erratum occurs, power consumption under lightly loaded conditions may exceed expectations. Intel has not observed any functional failures associated with this erratum.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL040	Processor May Hang When Both Threads are Active on A Physical Core
Problem	Under complex micro-architectural conditions, both logical processors on the same physical core may hang, with an internal timeout error (MCACOD 0400H) logged into IA32_MC3_STATUS (MSR 40DH). This erratum can only happen when both logical processors on the same physical core are active.
Implication	Due to this erratum, the processor may hang. Intel has not observed this erratum with any commercially available software.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL041	Processor May Hang During High-Throughput Graphics Scenarios
Problem	Running high graphics throughput workloads with corresponding high ring frequencies may lead to system failure
Implication	Due to this erratum, the system may hang when running high-throughput graphics scenarios such as graphics stress testing.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL042	PROCHOT De-assertion May Lead to False Processor LFM
Problem	The processor may miscount consecutive PROCHOT assertions, which may lead to an extended duration for lowest P-state operation.
Implication	PROCHOT demotion algorithm may put the processor in LFM for longer than expected.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL043	Some Errors Logged in IA32_MC1_STATUS May Not Generate Machine Check Exceptions
Problem	Some errors may be logged in IA32_MC1_STATUS MSR (405H) without generating #MC (machine check exception). The logged errors would have the VAL bit set to 1 (bit 63), UC bit set to 1 (bit 61), PCC bit set to 1 (bit 57) and EN bit set to 0 (bit 60). These errors may be: 1. Spurious errors, which do not affect the system behavior. In such cases IA32_MC1_STATUS will have MCACOD (bits[15:0]) equal to 401H and MSCOD (bits[31:16]) equal to 20H. 2. Illegal software behavior, in the context of APIC (advanced programmable interrupt controller) access, which includes errors that result from mapping the APIC to non-UC (uncatchable) memory type, or trying to access the APIC memory using illegal access size (larger than 4 bytes). APIC memory is defined by IA32_APIC_BASE MSR (1BH). These cases will have the same values logged into IA32_MC1_STATUS as the spurious errors. 3. In extreme rare cases these errors may be real errors which could lead to unpredictable system behavior.
Implication	Errors may be logged in IA32_MC1_STATUS MSR with EN bit set to 0. Software that incorrectly ignores the EN bit value may interpret these errors as fatal events. Software that properly interprets EN bit may fail to behave as expected.
Workaround	None identified.

Status	For the steppings affected, refer to the Summary Table of Changes.

ICL044	**The Processor May Assert THRMTRIP#**
Problem	When the processor exits a PKG-C9/C10 exit, it may incorrectly assert THRMTRIP# signal.
Implication	Due to this erratum, THRMTRIP# may be asserted and the system may hang.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL045	**Placing Page Table Information in the APIC-Access Page May Lead to Unexpected Page Faults While Performing Enclave Accesses**
Problem	Guest-physical access using a guest-physical address that translates to an address on the APIC-access page (as identified by the APIC-access address field in the VMCS) should cause an APIC-access VM exit. This includes page table information accesses done as part of page translation (page walks). Due to this erratum placing page table information in the APIC-access page may result in a page fault instead of VM exit when the page translation is done as part of an enclave access.
Implication	Software that places page table information in the APIC access page may get page faults on executing enclave accesses, instead of exiting to the VMM (Virtual-Machine Monitor). Intel has not observed this erratum with any commercially available software.
Workaround	Software should not place page table information in the APIC access page.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL046	**Instruction Fetch May Cause Machine Check If Page Size Was Changed without Invalidation**
Problem	This erratum may cause a machine-check error (IA32_MCi_STATUS.MCACOD=0150H) on the fetch of an instruction. It applies only if (1) instruction bytes are fetched from a linear address translated using a 4-Kbyte page and cached in the processor; (2) the paging structures are later modified so that these bytes are translated using a large page (2-Mbyte, 4-Mbyte or 1-GByte) with a different physical address or memory type; and (3) the same instruction is fetched after the paging structure modification but before software invalidates any TLB entries for the linear region.
Implication	Due to this erratum an unexpected machine check with error code 0150H with MSCOD 00FH may occur, possibly resulting in a shutdown. This erratum could also lead to unexpected correctable machine check (IA32_MCi_STATUS.UC=0) with error code 005H with MSCOD 00FH.
Workaround	Software should not write to a paging-structure entry in a way that would change the page size and either the physical address, memory type or User/Supervisor bit. It can instead use one of the following algorithms: first clear the P flag in the relevant paging-structure entry (example: PDE); then invalidate any translations for the affected linear addresses; and then modify the relevant paging-structure entry to set the P flag and establish the new page size. An alternative algorithm: first change the physical page attributes (combination of physical address, memory type and User/Supervisor bit) in all 4K pages in the affected linear addresses; then invalidate any translations for the affected linear addresses; and then modify the relevant paging-structure entry to establish the new page size.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL047	System May Hang When Graphics Core is Running in Low Frequency Mode
Problem	When the Graphics core is running in low frequency, the system may hang, resulting in an Internal Timer Error machine check exception.
Implication	Due to this erratum, a system hang may occur resulting in an unexpected machine check with error code MCACOD=400h.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL048	USB 3.x Devices May Not Enumerate or May Downgrade to USB2 Speeds on Ports Without a Retimer
Problem	LFPS (Low Frequency Periodic Signaling) sampling may fail when hot plugging on USB3.x ports without a retimer.
Implication	USB3.x device may not enumerate or may downgrade to USB2 speed.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL049	Isochronous Devices May Experience Deferred Memory Accesses
Problem	If accesses to certain Display Engine configuration registers occur while the Display Engine is in a low power state, these requests may take longer than expected.
Implication	When this erratum occurs, isochronous devices may experience deferred memory access, leading to, for example, audio artifacts such as popping, clicking, or hissing.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL050	FIVR PS5 Insufficient Current During PKG-C6 Resume
Problem	FIVR PS5 (Power State 5) current may be insufficient during PKG-C6 resume.
Implication	System implication is design dependent which may lead to system instability or display flicker during PKG-C6 resume.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL051	LPDDR4x May Incorrectly Exit Self-Refresh
Problem	During PKG-C7 entry an improper control logic power sequence may cause an incorrect pulse to occur on LPDDR4x CKE, due to incorrect DDR IO configurations.
Implication	Due to this erratum DRAM may incorrectly exit self-refresh, resulting in unpredictable system behavior.
Workaround	A fix for this erratum is available in BIOS. (BIOS version 3512 and SiC version 08.00.57.10)
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL052	Incorrect TCSS DTS When A Thunderbolt™ Device Is Connected
Problem	When a high-performance Thunderbolt™ device is connected to Type-C port 3 or 4 the TCSS DTS may be incorrectly calculated.
Implication	Due to this erratum, TJMAX may be exceeded leading to unpredictable system behavior or a global reset.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL053	REP MOVSB Instruction to Or from A Non-flat Segment May Cause Unpredictable System Behavior
Problem	Under complex micro-architectural conditions, using a REP MOVSB instruction in which at least one of the operands (destination or source) of the instruction is in a non-flat segment mode, might cause unpredictable system behavior.
Implication	Due to this erratum, unpredictable system behavior may occur. Intel has not observed this erratum with any commercially available software.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL054	MASKMOV* Instruction to A Physical Memory Location Mapped by Two Linear Addresses of Different Page Sizes May Result in Unpredictable System Behavior
Problem	Under complex microarchitectural conditions, executing a MASKMOVQ or MASKMOVDQU instruction to a physical memory location mapped by two linear addresses of different page sizes pages may result in unpredictable system behavior if either accessed flag (A flag) or the dirty flag (D flag) of one of those pages are cleared or the transaction is to a uncacheable memory.
Implication	When this erratum occurs, the system may behave unpredictably. Intel has not observed this erratum with any commercially available software.
Workaround	Software that uses MASKMOVQ or MASKMOVDQU instructions should invalidate the TLB entries (using an INVLPG instruction) containing an address that could be accessed as part of two different page sizes after each paging-structure change that affects those pages
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL055	USB 3.x Link Training Failure
Problem	USB 3.x link training may fail in systems with a retimer due to incorrect Rcomp value.
Implication	Due to this erratum, some USB3.x devices may not be functional until unplugged and reconnected and/or requiring a system reset.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL056	VTd DMA Remapping Disable in Gfx IOMMU May Cause Display Artifacts or Flickering
Problem	If system software enables VTd translations for the Gfx IOMMU (TE=1) and then switches the Gfx IOMMU to disable translations (TE=0) while the display is enabled, display memory underrun condition can occur.
Implication	Due to this erratum, momentary display corruption may occur. Intel has only observed this issue when BIOS pre-boot DMA protection was enabled for Gfx IOMMU.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL057	MDS_NO Bit in IA32_ARCH_CAPABILITIES MSR is Incorrectly Set
Problem	MDS_NO bit (bit 5) in IA32_ARCH_CAPABILITIES MSR (10Ah) is set, incorrectly indicating full activation of all MDS (micro-architectural data sampling) mitigations.
Implication	Due to this erratum, the IA32_ARCH_CAPABILITIES MDS_NO bit incorrectly reports the activation of all MDS mitigations actions.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL058	Overflow Flag in IA32_MC0_STATUS MSR May be Incorrectly Set
Problem	Under complex micro-architectural conditions, a single internal parity error seen in IA32_MC0_STATUS MSR (401h) with MCACOD (bits 15:0) value of 5h and MSCOD (bits 31:16) value of 7h, may set the overflow flag (bit 62) in the same MSR.
Implication	Due to this erratum, the IA32_MC0_STATUS overflow flag may be set after a single parity error. Intel has not observed this erratum with any commercially available software.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL059	IA32_L3_QOS_Mask_N Accepts Non-Contiguous Masks
Problem	Non-contiguous capacity masks set in the IA32_L3_QOS_Mask_N MSRs (address c90h through c9fh) will not cause #GP (general protection) as expected.
Implication	Due to this erratum, the processor will not report a #GP when non-contiguous capacity masks are set in the IA32_L3_QOS_Mask_N MSRs.
Workaround	Software should not expect a #GP after setting non-contiguous capacity masks in IA32_L3_QOS_Mask_N MSRs.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL060	System May Hang When CR0.TS Or CR0.EM Are Set
Problem	Under complex micro-architectural conditions, when either CR0.TS (bit 3) or CR0.EM (bit 2) are set, both logical processors on the same physical core may hang, with an internal timeout error (MCACOD 0400H) logged into IA32_MC3_STATUS (MSR 40DH). This can only happen when both logical processors on the same physical core are active.

Implication	Due to this erratum, system may hang.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL061	**Processor May Experience Unexpected System Behavior When CR0.TS Or CR0.EM Are Set**
Problem	Under complex microarchitectural conditions, when either CR0.TS (bit 3) or CR0.EM (bit 2) are set, unexpected system behavior may occur.
Implication	Due to this erratum, the processor may experience unexpected system behavior.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL062	**Wrong Page Access Semantics May be Reported When Intel® SGX ENCLU[EMODPE] Instruction Generates Page Fault (#PF) Exception**
Problem	When Intel® SGX extends an Enclave Page Cache (EPC) via the page permissions instruction (ENCLU[EMODPE]) and generates a Page Fault (#PF), even though the page permissions instruction access is a read access to the target page, the Page Fault Error Code (#PF's PFEC) will indicate that the fault occurred on a write (PFEC.W bit will be set) instead.
Implication	This erratum may impact debugging Intel® SGX enclaves software. Intel has not observed this erratum with any commercially available software.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL063	**Usage of Bit 55 of IA32_TSC_DEADLINE MSR May Cause Spurious Timer Interrupt**
Problem	When using the APIC timer in Time Stamp Counter Deadline (TSC-deadline) mode, if the most significant set bit in the written value to the TSC-Deadline MSR is bit 55, the processor may generate a spurious timer interrupt.
Implication	When this erratum occurs, a spurious timer interrupt may occur causing unpredictable system behavior. Intel has not observed this erratum with any commercially available software.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL064	**Time Stamp Counters May Contain A Shifted Time Value**
Problem	Under complex micro-architectural conditions, the processor's RDTSC and RDTSCP instructions may report a shifted value. In these cases, the shift value will be larger than a minute.
Implication	Software may experience a non-monotonic time stamp counter, misalignment across threads, or a spurious timer interrupt.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL065	Unpredictable System Behavior Due to Move Elimination
Problem	Under complex micro-architectural conditions, when Move Elimination is performed, unpredictable system behavior may occur.
Implication	Due to this erratum, unpredictable system behavior may occur.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL066	REP MOVSB Might Lead to Incorrect ESP
Problem	Under complex micro-architectural conditions, using the REP MOVSB instruction may lead to an incorrect value in the Extended Stack Pointer (ESP) register. This can only happen when both logical processors on the same physical core are active.
Implication	Due to this erratum, the Extended Stack Pointer register may be incorrect, leading to unpredictable system behavior.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL067	A Ring Interconnect Performance State Transition May Result in Unpredictable System Behavior
Problem	Under a complex set of micro-architectural conditions, an incorrect sequence of operations during a ring interconnect performance state transition may result in unpredictable system behavior.
Implication	Due to this erratum, unpredictable system behavior may occur.
Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL068	Uncore Performance Monitoring Controls May Not Function Properly
Problem	MSR_UNC_PERF_GLOBAL_CTRL (E01H) (bit29) 'Enable all uncore counters' and (bit 31) 'Freeze counters' may not function. In addition, MSR_UNC_ARB_PERFCTR0_0 (3B0H) and MSR_UNC_ARB_PERFEVTSEL0_0 (3B2H) may not return correct values.
Implication	Due to this erratum, software cannot globally control uncore performance counters using MSR_UNC_PERF_GLOBAL_CTRL and cannot use MSR_UNC_ARB_PERFCTR0_0 or MSR_UNC_ARB_PERFEVTSEL0_0.
Workaround	None identified. Software will need to utilize each individual local enable (bit 22) in the specific uncore PMON Performance Event Select (PERFEVTSEL) registers.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL069	A Memory Controller Domain Low Power Mode Transition May Result in Retrieval of Incorrect Data from Memory
Problem	Under a complex set of micro-architectural conditions, Memory Controller domain low power mode state transition may result in retrieval of incorrect data from memory.
Implication	Due to this erratum, unexpected system behavior may occur.

Workaround	It is possible for the BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL070	**VT-d Domain-Specific Context Cache Invalidation Requests May Not Complete**
Problem	The VT-d architecture allows software to issue Domain- or Device- specific Context Cache invalidation requests. In such cases, the VT-d engine is expected to invalidate all entries that belong to the Domain (or Device) from Context cache. Due to this errata, some Context Cache entries that were required to be invalidated are not invalidated. Global context cache invalidation will correctly invalidate all entries of the context cache.
Implication	Incomplete VT-d Domain-specific Content Cache Invalidation may lead to unpredictable system behavior.
Workaround	It is possible for BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL071	**Type-C Ports Configured as DP-FIXD May Lead to System Hang**
Problem	When the processor attempts to enter a deep power state, on platforms with all enabled Type-C ports configured as DP-FIXD (HDMI/DP) with no devices attached on any port, the system may hang.
Implication	Due to this erratum, the system may hang.
Workaround	It is possible for a BIOS code change to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL072	**VERR Instruction Inside VM-entry May Cause DR6 to Contain Incorrect Values**
Problem	Under complex micro-architectural conditions, a VERR instruction that follows a VM-entry with a guest state indicating MOV SS blocking (bit 1 in the Interruptibility state) and at least one of B3-B0 bits set (bits 3:0 in the pending debug exception), may lead to incorrect values in DR6.
Implication	Due to this erratum, DR6 may contain incorrect values. Intel has not observed this erratum with any commercially available software.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL073	**Processor May Hang if Warm Reset Triggers During BIOS Initialization**
Problem	Under complex micro-architectural conditions, when the processor receives a warm reset during BIOS initialization, the processor may hang with a machine check error reported in IA32_MCi_STATUS, with MCACOD (bits [15:0]) value of 0400H, and MSCOD (bits [31:16]) value of 0080H.
Implication	Due to this erratum, the processor may hang. Intel has only observed this erratum in a synthetic test environment.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL074	N/A. Erratum has been Removed.

ICL075	IA32_RTIT_STATUS.FilterEn Bit Might Reflect A Previous Value
Problem	Under complex micro-architectural conditions, reading the IA32_RTIT_STATUS.FilterEn bit (bit 0 in MSR 571h) after entering or exiting an RTIT region might reflect a previous value instead of the current one.
Implication	Due to this erratum, IA32_RTIT_STATUS.FilterEn bit might reflect a previous value. This erratum has not been seen in any commercially available software.
Workaround	Software should perform an LFENCE instruction prior to reading the IA32_RTIT_STATUS MSR to avoid this issue.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL076	SSBD May Not Properly Restrict Load Execution
Problem	The Speculative Store Bypass Disable (SSBD) (IA32_SPEC_CTRL MSR 48h, bit [2]) capability should prevent loads from executing speculatively before the addresses of all older stores are known. SMM and SGX enclave always apply this policy. Under certain complex microarchitectural conditions, speculative loads may execute before all older stores are known when in SMM or SGX or when SSBD control bit is set.
Implication	Due to this erratum, the speculation properties implied by SSBD may not be fully met. Intel has not observed any functional implications due to this erratum.
Workaround	It is possible for BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL077	Executing an XSAVE or VZEROALL Instruction After SYSENTER May Result in Unexpected SSE/AVX Register Values
Problem	Under complex microarchitectural conditions, executing any of the XSAVE, XSAVEOPT, XSAVEC, XSAVES, or VZEROALL instructions shortly after the execution of SYSENTER may result in unexpected SSE/AVX register values.
Implication	Due to this erratum, software may observe unexpected values in the SSE/AVX registers. Intel has only observed this erratum in a synthetic test environment.
Workaround	None identified. An operating system's SYSENTER handler should avoid using executing an XSAVE or VZEROALL instruction in its first ten instructions.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL078	False MC1 Error Reported in The Shadow of an Internal Timer Error
Problem	After an internal timer error has been reported in MC3_STATUS MSR (0x40d) with MCACOD (bits [15:0]) value of 0400H, and MSCOD (bits [31:16]) value of 0080H, under complex micro-architectural conditions, a false error may be reported in MC1_STATUS MSR (0x405) with MCACOD 0x174 or MCACOD 0x124.
Implication	Due to this erratum, a false MCE may be reported in MC1_STATUS MSR. Intel has only observed this erratum in a synthetic test environment.

Workaround	Software should ignore the MC1_STATUS error when it appears with an internal timer error.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL079	**Placing Posted-Interrupt Descriptors Within the PRMRR May Result in a Processor Hang**
Problem	Posted-interrupt processing is a virtualization feature for interrupts which requires configuring addresses in the posted-interrupt descriptor fields in the VMCS (Virtual Machine Control Structure). Configuring posted-interrupt descriptors addresses that are within the PRMRR (Processor Reserved Memory Range Register, defined by MSR 1F4H and MSR 1F5H) may result in a logical processor hang.
Implication	This erratum may result in a processor hang. Intel has not observed this erratum with any commercially available software.
Workaround	VMM (Virtual Machine Monitor) software should not use addresses within the PRMRR for posted-interrupt descriptors.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL080	**System May Experience an Internal Timeout Error When Directing Intel® PT to a Small, Uncacheable, Single-Range Output Buffer**
Problem	A processor hang may result if Intel® Processor Trace (Intel® PT) is enabled with Mini Time Counter (MTC) packets and single range output mode (TraceEn[0]=1, MTCEn[9]=1 and ToPA[8]=0 in IA32_RTIT_CTL MSR (0570h)), while the output buffer is less than 1 KB in size (IA32_RTIT_OUTPUT_MASK_PTRS[31:0] MSR (0561h) < 0400h) and it is mapped as uncacheable (UC) or write protect (WP) memory type in the Memory Type Range Registers (MTRRs).
Implication	Due to this erratum, the system may experience an Internal Timer Error Machine Check (IA32_MCi_STATUS.MCACOD=400H; bits 15:0). Intel has only observed this erratum in a synthetic test environment.
Workaround	Avoid directing Intel PT output to an uncacheable buffer less than 1KB in size.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL081	**Setting MISC_FEATURE_CONTROL.DISABLE_THREE_STRIKE_CNT Does Not Prevent the Three-strike Counter from Incrementing**
Problem	Setting MISC_FEATURE_CONTROL.DISABLE_THREE_STRIKE_CNT (bit 11 in MSR 1A4h) does not prevent the three-strike counter from incrementing as documented; instead, it only prevents the signaling of the three-strike event once the counter has expired.
Implication	Due to this erratum, software may be able to see the three-strike logged in the MC3_STATUS (MSR 40Dh, MCACOD = 400h [bits 15:0]) even when MISC_FEATURE_CONTROL.DISABLE_THREE_STRIKE_CNT is set.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL082	Intel® PT Trace May Contain Incorrect Data When Configured With Single Range Output Larger Than 4KB
Problem	Under complex micro-architectural conditions, when using Intel® Processor Trace (Intel® PT) with single range output larger than 4KB, disabling PT and then enabling PT using the TraceEn bit in IA32_RTIT_CTL MSR (MSR 570h, bit 0) may cause incorrect output values to be recorded.
Implication	Due to this erratum, a PT trace may contain incorrect values.
Workaround	None identified. Software should avoid using PT with single range output larger than 4KB.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL083	Incorrect MCACOD For L2 Prefetch MCE
Problem	Under complex micro-architectural conditions, an L2 prefetch MCE that should be reported with MCACOD 165h in IA32_MC3_STATUS MSR (MSR 40dh, bits [15:0]) may be reported with an MCACOD of 101h.
Implication	Due to this erratum, the reported MCACOD for this MCE may be incorrect.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL084	Call Instruction Wrapping Around The 32-bit Address Boundary May Return to Incorrect Address
Problem	In 32-bit mode, a call instruction wrapping around the 32-bit address should save a return address near the bottom of the address space (low address) around address zero. Under complex micro-architectural conditions, a return instruction following such a call may return to the next sequential address instead (high address).
Implication	Due to this erratum, In 32-bit mode a return following a call instruction that wraps around the 32-bit address boundary may return to the next sequential IP without wrapping around the address, possibly resulting in a #PF. Intel has not observed this behavior on any commercially available software.
Workaround	Software should not place call instructions in addresses that wrap around the 32-bit address space in 32-bit mode.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL085	Branch Predictor May Produce Incorrect Instruction Pointer
Problem	Under complex microarchitectural conditions, the branch predictor may produce an incorrect instruction pointer leading to unpredictable system behavior.
Implication	Due to this erratum, the system may exhibit unpredictable behavior.
Workaround	It may be possible for BIOS to contain a workaround for this erratum.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL086	USB 3.2 DbC Sublink Speed Attribute ID (SSID) Value
Problem	The USB 3.2 Debug Class Device (DbC) reports an incorrect Sublink Speed Attribute ID (SSID) value in the SuperSpeedPlus USB Device Capability field.
Implication	Due to this erratum, the processor USB 3.2.DbC (Debug Capability) device may fail to enumerate when connected to a USB 3.2 Gen 2x1 port.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

ICL087	A Write to The TSC_Deadline MSR May Cause an Unexpected Timer Interrupt
Problem	Under complex micro-architectural conditions, writing a non-zero value to the Time-Stamp Counter (TSC) Deadline counter, IA32-TSC_DEADLINE MSR (6E0h), may cause timer interrupt following the write.
Implication	Due to this erratum, an unexpected timer interrupt may be signaled.
Workaround	None identified.
Status	For the steppings affected, refer to the Summary Table of Changes.

§ §

Specification Changes

ID	Affected Products/Steps	Specification Change Title	Issue	Previous Text Reference	New Text	Affected Document(s)
001	U D1	PKG-C9 disabled	System may hang when resuming from PKG-C9	The processor supports C0, C2, C3, C6, C7, C8, C9, and C10 package states	N/A	341077
002	U/Y D1	FIVR Power state 5 (PS5) disabled	FIVR PS5 Insufficient Current During PKG-C6 Resume	N/A	N/A	341077

Note: There are no Specification Clarifications or Document Changes for this revision of the specification update.

§ §