

Mobile 4th Generation Intel[®] Core[™] Processor Family, Mobile Intel[®] Pentium[®] Processor Family, and Mobile Intel[®] Celeron[®] Processor Family

Specification Update

Supporting 4th Generation Intel[®] Core[™] Processor based on Mobile M-Processor and H-Processor Lines

Supporting 4th Generation Intel[®] Core[™] Processor based on Mobile U-Processor and Y-Processor Lines

April 2020

Revision 038US



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.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at Intel.com, or from the OEM or retailer.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

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.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

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

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

Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit: <http://www.intel.com/go/Virtualization>.

Intel® Turbo Boost Technology requires a system with Intel® Turbo Boost Technology. Intel Turbo Boost Technology and Intel Turbo Boost Technology 2.0 are only available on select Intel® processors. Consult your PC manufacturer. Performance varies depending on hardware, software, and system configuration. For more information, visit: <http://www.intel.com/go/turbo>.

Intel® Hyper-Threading Technology requires an Intel® HT Technology enabled system, check with your PC manufacturer. Performance will vary depending on the specific hardware and software used. Not available on Intel® Core™ i5-750. For more information including details on which processors support HT Technology, visit <http://www.intel.com/info/hyperthreading>.

Intel® 64 architecture requires a system with a 64-bit enabled processor, chipset, BIOS and software. Performance will vary depending on the specific hardware and software you use. Consult your PC manufacturer for more information. For more information, visit: <http://www.intel.com/info/em64t>.

Intel, Intel Core, Intel386, Intel486, Pentium, Celeron, and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2020, Intel Corporation. All rights reserved.



Contents

Revision History	4
Preface	7
Summary Tables of Changes	9
Identification Information	18
Errata	24
Specification Changes	72
Specification Clarifications	73
Documentation Changes	74

§ §



Revision History

Revision	Description	Date
001	Initial Release.	June 2013
002	Revision number skipped.	N/A
003	- Errata - Added D-0 stepping to errata summary table - Added HSM60-106 - Updated Identification Information	August 2013
004	Revision number skipped.	N/A
005	- Errata - Moved previous HSM106 to HSM116 - Added HSM106-115 and HSM117-125 - Processor Identification - Updated Table 3, Processor Identification by Register Contents - Updated Table 4, 4th Generation Intel® Core™ Processor based on Mobile M-Processor and H-Processor Lines Processor Identification - Updated Table 5, 4th Generation Intel® Core™ Processor based on Mobile U-Processor and Y-Processor Lines Processor Identification	November 2013
006	- Identification Information - Updated Table 5, 4th Generation Intel® Core™ Processor based on Mobile U-Processor and Y-Processor Lines Processor Identification	December 2013
007	- Errata - Added HSM126-128	December 2013
008	- Errata - Added HSM129-131	January 2014
009	- Errata - Added HSM132-133 - Updated Table 3, Processor Identification by Register Contents	February 2014
010	- Added 4th Generation Intel® Core™ processor based on Mobile H-Processor Line (BGA) with GT3 Graphics - Errata - Modified HSM30 - Added HSM134 - Updated Table 3, Processor Identification by Register Contents	March 2014
011	- Errata - Added HSM135-139 - Identification Information - Updated Table 3, Processor Identification by Register Contents - Updated Table 4, 4th Generation Intel® Core™ Processor based on Mobile M-Processor and H-Processor Lines Processor Identification - Updated Table 5, 4th Generation Intel® Core™ Processor based on Mobile U-Processor and Y-Processor Lines Processor Identification	April 2014
012	- Errata - Added HSM140-142	June 2014



Revision	Description	Date
013	- Errata - Added HSM143 - Removed HSM76, HSM92, HSM124, HSM140 - Identification Information - Updated Processor Identification tables.	July 2014
014	Revision number skipped.	N/A
015	- Errata - Modified HSM142 - Added HSM144-150 - Specification Changes - Added HSM1 - Identification Information - Updated Processor Identification tables.	August 2014
016	Revision number skipped.	N/A
017	- Errata - Added HSM151-152	October 2014
018	- Errata - Added HSM153-154	November 2014
019	- Errata - Modified HSM153 - Identification Information - Updated Table 4, 4th Generation Intel® Core™ Processor based on Mobile M-Processor and H-Processor Lines Processor Identification	December 2014
020	- Errata - Modified HSM34 - Added HSM155	January 2015
021	- Errata - Added HSM156-158	February 2015
022	- Errata - Added HSM159	March 2015
023	Revision number skipped.	N/A
024	Revision number skipped.	N/A
025	- Errata - Added HSM160-162	August 2015
026	Revision number skipped.	N/A
027	- Errata - Added HSM163 - Updated Component Identification Table	October 2015
028	- Errata - Added HSM164-165	November 2015
029	- Errata - Added HSM166	January 2016
030	- Errata - Revised HSM160 Problem Statement - Added Errata HSM167 through HSM172	April 2016
031	- Errata - Revised HSM56 - Added Errata HSM173 and HSM174	May 2016



Revision History

Revision	Description	Date
032	• Errata — Removed HSM64 — Corrected Errata HSM95 and HSM96 titles — Added Errata HSM 175	June 2016
033	• Errata — Revised Errata HSM173 — Added Errata HSM176	July 2016
034	• Errata — Added Errata HSM177	August 2016
035	• Errata — Updated Errata HSM26 — Updated Errata HSM146 — Added Errata HSM178 through HSM182	January 2017
036	• Errata — Removed Errata HSM13 — Added Errata HSM183	March 2017
037	• Errata — Added Errata HSM184 — Added Errata HSM185	January 2020
038	• Errata — Added Errata HSM186 — Added Errata HSM187	April 2020



Preface

This document is an update to the specifications contained in the [Affected Documents](#) table below. This document is a compilation of device and documentation errata, specification clarifications and changes. It is intended for hardware system manufacturers and software developers of applications, operating systems, or tools.

Information types defined in [Nomenclature](#) are consolidated into the specification update and are no longer published in other documents.

This document may also contain information that was not previously published.

Affected Documents

Document Title	Document Number
Mobile 4th Generation Intel® Core™ Processor Family, Mobile Intel® Pentium® Processor Family, and Mobile Intel® Celeron® Processor Family Datasheet – Volume 1 of 2 Subtitle: Supporting 4th Generation Intel® Core™ Processor based on Mobile M-Processor and H-Processor Lines Supporting Mobile Intel® Pentium® Processor and Mobile Intel® Celeron® Processor Families	328901
Mobile 4th Generation Intel® Core™ Processor Family, Mobile Intel® Pentium® Processor Family, and Mobile Intel® Celeron® Processor Family Datasheet – Volume 2 of 2 Subtitle: Supporting 4th Generation Intel® Core™ Processor based on Mobile M-Processor and H-Processor Lines Supporting Mobile Intel® Pentium® Processor and Mobile Intel® Celeron® Processor Families	328902
Mobile 4th Generation Intel® Core™ Processor Family, Mobile Intel® Pentium® Processor Family, and Mobile Intel® Celeron® Processor Family Datasheet – Volume 1 of 2 Subtitle: Supporting 4th Generation Intel® Core™ Processor based on Mobile U-Processor and Y-Processor Lines Supporting Mobile Intel® Pentium® Processor and Mobile Intel® Celeron® Processor Families	329001
Mobile 4th Generation Intel® Core™ Processor Family, Mobile Intel® Pentium® Processor Family, and Mobile Intel® Celeron® Processor Family Datasheet – Volume 2 of 2 Subtitle: Supporting 4th Generation Intel® Core™ Processor based on Mobile U-Processor and Y-Processor Lines Supporting Mobile Intel® Pentium® Processor and Mobile Intel® Celeron® Processor Families	329002

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/content/www/us/en/support/processors/desktop-processors/000006715.html?wapkw=intel%20ae+64+and+ia-32+architectures+software+developer%20ca%209s+manual%3a



Document Title	Document Number / Location
Intel® 64 and IA-32 Architectures Software Developer's Manual Documentation Changes	https://software.intel.com/sites/default/files/managed/3e/79/252046-sdm-changed-document.pdf
ACPI Specifications	www.acpi.info

Nomenclature

Errata are design defects or errors. These may cause the processor 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.

S-Spec Number is a five-digit code used to identify products. Products are differentiated by their unique characteristics such as, core speed, L2 cache size, package type, etc. as described in the processor identification information table. Read all notes associated with each S-Spec number.

Specification Changes are modifications to the current published specifications. These changes will be incorporated in any new release of the specification.

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

Documentation Changes include typos, errors, or omissions from the current published specifications. These will be incorporated in any new release of the specification.

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, and so on).



Summary Tables of Changes

The following tables indicate the errata, specification changes, specification clarifications, or documentation changes which apply to the processor. Intel may fix some of the errata in a future stepping of the component, and account for the other outstanding issues through documentation or specification changes as noted. These tables use the following notations.

Codes Used in Summary Tables

Stepping

X: Errata exist in the stepping indicated. Specification Change or Clarification that applies to this stepping.

(No mark) or

(Blank box): This erratum is fixed in listed stepping or specification change does not apply to listed stepping.

Page

(Page): Page location of item in this document.

Status

Doc: Document change or update will be implemented.

Plan Fix: This erratum may be fixed in a future stepping of the product.

Fixed: This erratum has been previously fixed.

No Fix: There are no plans to fix this erratum.

Row

Change bar to left of a table row indicates this erratum is either new or modified from the previous version of the document.



Errata (Sheet 1 of 7)

Number	Steppings		Status	ERRATA
	C-0	D-0		
HSM1	X	X	No Fix	LBR, BTS, BTM May Report a Wrong Address when an Exception/Interrupt Occurs in 64-bit Mode
HSM2	X	X	No Fix	EFLAGS Discrepancy on Page Faults and on EPT-Induced VM Exits after a Translation Change
HSM3	X	X	No Fix	MCi_Status Overflow Bit May Be Incorrectly Set on a Single Instance of a DTLB Error
HSM4	X	X	No Fix	LER MSRs May Be Unreliable
HSM5	X	X	No Fix	MONITOR or CLFLUSH on the Local XAPIC's Address Space Results in Hang
HSM6	X	X	No Fix	An Uncorrectable Error Logged in IA32_CR_MC2_STATUS May also Result in a System Hang
HSM7	X	X	No Fix	#GP on Segment Selector Descriptor that Straddles Canonical Boundary May Not Provide Correct Exception Error Code
HSM8	X	X	No Fix	FREEZE_WHILE_SMM Does Not Prevent Event From Pending PEBS During SMM
HSM9	X	X	No Fix	APIC Error "Received Illegal Vector" May be Lost
HSM10	X	X	No Fix	Changing the Memory Type for an In-Use Page Translation May Lead to Memory-Ordering Violations
HSM11	X	X	No Fix	Performance Monitor Precise Instruction Retired Event May Present Wrong Indications
HSM12	X	X	No Fix	CR0.CD Is Ignored in VMX Operation
HSM13	X	X	No Fix	N/A. Erratum has been removed
HSM14	X	X	No Fix	Execution of VAESIMC or VAESKEYGENASSIST With An Illegal Value for VEX.vvvv May Produce a #NM Exception
HSM15	X	X	No Fix	Processor May Fail to Acknowledge a TLP Request
HSM16	X	X	No Fix	Interrupt From Local APIC Timer May Not Be Detectable While Being Delivered
HSM17	X	X	No Fix	PCIe* Root-port Initiated Compliance State Transmitter Equalization Settings May be Incorrect
HSM18	X	X	No Fix	PCIe* Controller May Incorrectly Log Errors on Transition to RxL0s
HSM19	X	X	No Fix	Unused PCIe* Lanes May Report Correctable Errors
HSM20	X	X	No Fix	Accessing Physical Memory Space 0-640K through the Graphics Aperture May Cause Unpredictable System Behavior
HSM21	X	X	No Fix	PCIe Root Port May Not Initiate Link Speed Change
HSM22	X	X	No Fix	Pending x87 FPU Exceptions (#MF) May be Signaled Earlier Than Expected
HSM23	X	X	No Fix	DR6.B0-B3 May Not Report All Breakpoints Matched When a MOV/POP SS is Followed by a Store or an MMX Instruction
HSM24	X	X	No Fix	VEX.L is Not Ignored with VCVT*2SI Instructions
HSM25 ¹	X	X	No Fix	Processor May Shut Down During Boundary Scan Testing
HSM26	X	X	No Fix	Some DRAM and L3 Cache Performance Monitoring Events May Count Incorrectly
HSM27	X	X	No Fix	Specific Graphics Blitter Instructions May Result in Unpredictable Graphics Controller Behavior
HSM28	X	X	No Fix	Processor May Enter Shutdown Unexpectedly on a Second Uncorrectable Error



Errata (Sheet 2 of 7)

Number	Steppings		Status	ERRATA
	C-0	D-0		
HSM29 ²	X	X	No Fix	Modified Compliance Patterns for 2.5 GT/s and 5 GT/s Transfer Rates Do Not Follow PCIe* Specification
HSM30	X	X	No Fix	Performance Monitor Counters May Produce Incorrect Results
HSM31	X	X	No Fix	Performance Monitor UOPS_EXECUTED Event May Undercount
HSM32	X	X	No Fix	MSR_PERF_STATUS May Report an Incorrect Core Voltage
HSM33 ²	X	X	No Fix	PCIe* Atomic Transactions From Two or More PCIe Controllers May Cause Starvation
HSM34	X	X	No Fix	The Corrected Error Count Overflow Bit in IA32_MCO_STATUS is Not Updated When The UC Bit is Set
HSM35	X	X	No Fix	An AVX Gather Instruction That Causes an EPT Violation May Not Update Previous Elements
HSM36	X	X	No Fix	PLATFORM_POWER_LIMIT MSR Not Visible
HSM37	X	X	No Fix	LPDDR Memory May Report Incorrect Temperature
HSM38	X	X	No Fix	PCIe* Host Bridge DID May Be Incorrect
HSM39	X	X	No Fix	TSC May be Incorrect After a Deep C-State Exit
HSM40 ²	X	X	No Fix	PCIe* Controller May Initiate Speed Change While in DL_Init State Causing Certain PCIe Devices to Fail to Train
HSM41	X	X	No Fix	Spurious VT-d Interrupts May Occur When the PFO Bit is Set
HSM42	X	X	No Fix	N/A. Erratum has been removed
HSM43	X	X	No Fix	AVX Gather Instruction That Causes a Fault or VM Exit May Incorrectly Modify Its Destination Register
HSM44	X	X	No Fix	Inconsistent NaN Propagation May Occur When Executing (V)DPSS Instruction
HSM45	X	X	No Fix	Display May Flicker When Package C-States Are Enabled
HSM46	X	X	No Fix	Certain Combinations of AVX Instructions May Cause Unpredictable System Behavior
HSM47	X	X	No Fix	Processor May Incorrectly Estimate Peak Power Delivery Requirements
HSM48	X	X	No Fix	IA32_PERF_CTL MSR is Incorrectly Reset
HSM49	X	X	No Fix	Processor May Hang During a Function Level Reset of the Display
HSM50	X	X	No Fix	AVX Gather Instruction That Should Result in #DF May Cause Unexpected System Behavior
HSM51	X	X	No Fix	Throttling and Refresh Rate Maybe be Incorrect After Exiting Package C-State
HSM52	X	X	No Fix	Processor May Livelock During On Demand Clock Modulation
HSM53	X	X	No Fix	IA32_DEBUGCTL.FREEZE_PERFMON_ON_PMI is Incorrectly Cleared by SMI
HSM54	X	X	No Fix	The From-IP for Branch Tracing May be Incorrect
HSM55	X	X	No Fix	TM1 Throttling May Continue indefinitely
HSM56	X	X	No Fix	Internal Parity Errors May Incorrectly Report Overflow in The IA32_MC2_STATUS MSR
HSM57	X	X	No Fix	Performance Monitor Events OTHER_ASSISTS.AVX_TO_SSE And OTHER_ASSISTS.SSE_TO_AVX May Over Count
HSM58	X	X	No Fix	Processor May Run at Incorrect P-State



Errata (Sheet 3 of 7)

Number	Steppings		Status	ERRATA
	C-0	D-0		
HSM59	X	X	No Fix	Performance Monitor Event DSB2MITE_SWITCHES.COUNT May Over Count
HSM60	X	X	No Fix	Performance Monitor Register UNC_PERF_GLOBAL_STATUS Not Restored on Package C7 Exit
HSM61	X	X	No Fix	Processor May Not Enter Package C6 or Deeper C-states When PCIe* Links Are Disabled
HSM62	X	X	No Fix	Performance Monitor Event For Outstanding Offcore Requests And Snoop Requests May Over Count
HSM63	X	X	No Fix	Some Performance Monitor Event Counts May be Inaccurate During SMT Mode
HSM64	X	X	No Fix	N/A. Errata has been Removed
HSM65	X	X	No Fix	The Upper 32 Bits of CR3 May be Incorrectly Used With 32-Bit Paging
HSM66	X	X	No Fix	Performance Monitor Events HLE_RETIRED.ABORTED_MISC4 And RTM_RETIRED.ABORTED_MISC4 May Over Count
HSM67 ²	X	X	No Fix	A PCIe* LTR Update Message May Cause The Processor to Hang
HSM68	X	X	No Fix	GETSEC Does Not Report Support For S-CRTM
HSM69	X	X	No Fix	EPT Violations May Report Bits 11:0 of Guest Linear Address Incorrectly
HSM70	X	X	No Fix	APIC Timer Might Not Signal an Interrupt While in TSC-Deadline Mode
HSM71	X	X	No Fix	IA32_VMX_VMCS_ENUM MSR (48AH) Does Not Properly Report The Highest Index Value Used For VMCS Encoding
HSM72	X	X	No Fix	Incorrect FROM_IP Value For an RTM Abort in BTM or BTS May be Observed
HSM73	X	X	No Fix	VT-d Hardware May Perform STRP And SIRTTP Operations on a Package C7 Exit
HSM74	X	X	No Fix	General-Purpose Performance Counters Can Unexpectedly Increment
HSM75	X	X	No Fix	Performance Monitoring Events May Report Incorrect Number of Load Hits or Misses to LLC
HSM76	X	X	No Fix	N/A. Erratum has been removed
HSM77	X	X	No Fix	Locked Load Performance Monitoring Events May Under Count
HSM78 ¹	X	X	No Fix	Processor May Hang Upon Entrance to Package C6 or C7
HSM79	X	X	No Fix	Graphics Processor Ratio And C-State Transitions May Cause a System Hang
HSM80	X	X	No Fix	Certain Performance Monitoring Events May Over Count Software Demand Loads
HSM81	X	X	No Fix	Accessing Nonexistent Uncore Performance Monitoring MSRs May Not Signal a #GP
HSM82 ¹	X	X	No Fix	Power and Performance Regulation May Vary When Using RAPL
HSM83	X	X	No Fix	Call Stack Profiling May Produce Extra Call Records
HSM84 ²	X	X	No Fix	Warm Reset May Fail or Lead to Incorrect Power Regulation
HSM85	X	X	No Fix	PCIe* Host Bridge DID May Be Incorrect
HSM86 ²	X	X	No Fix	Transactional Abort May Produce an Incorrect Branch Record
HSM87	X	X	No Fix	SMRAM State-Save Area Above the 4GB Boundary May Cause Unpredictable System Behavior



Errata (Sheet 4 of 7)

Number	Steppings		Status	ERRATA
	C-0	D-0		
HSM88 ¹	X	X	No Fix	TM1 Throttling Via IA32_CLOCK_MODULATION MSR May Hang
HSM89	X	X	No Fix	DMA Remapping Faults for the Graphics VT-d Unit May Not Properly Report Type of Faulted Request
HSM90 ¹	X	X	No Fix	Exiting Deep Package C-State May Result in a System Hang
HSM91	X	X	No Fix	AVX Gather Instructions Page Faults May Report an Incorrect Faulting Address
HSM92	X	X	No Fix	N/A. Erratum has been removed
HSM93	X	X	No Fix	Event Injection by VM Entry May Use an Incorrect B Flag for SS
HSM94 ¹	X	X	No Fix	LPDDR3 ZQ Calibration Following Deep Package C-state Exit May Lead to Unpredictable System Behavior
HSM95	X	X	No Fix	A Fault in SMM May Result in Unpredictable System Behavior
HSM96	X	X	No Fix	Processor Frequency is Unexpectedly Limited Below Nominal P1 When cTDP Down is Enabled
HSM97	X	X	No Fix	PMI May be Signaled More Than Once For Performance Monitor Counter Overflow
HSM98	X	X	No Fix	Execution of FXSAVE or FXRSTOR With the VEX Prefix May Produce a #NM Exception
HSM99	X	X	No Fix	RDRAND Execution in a Transactional Region May Cause a System Hang
HSM100 ¹	X	X	No Fix	Intel® Turbo Boost Technology May be Incorrectly Reported as Supported on Intel® Core™ i3 U-series, Y-series and select Pentium® processors
HSM101	X	X	No Fix	Uncore Clock Frequency Changes May Cause Audio/Video Glitches
HSM102 ²	X	X	No Fix	Processor May Experience a Spurious LLC-Related Machine Check During Periods of High Activity
HSM103	X	X	No Fix	The Processor May Not Enter Package C7 When Using a PSR Display
HSM104	X	X	No Fix	Video/Audio Distortion May Occur
HSM105	X	X	No Fix	System May Hang When Audio is Enabled During Package C3
HSM106	X	X	No Fix	INVPCID May Not Cause #UD in VMX Non-Root Operation
HSM107	X	X	No Fix	Non-Compliant PFAT Module Base Address May Cause Unpredictable System Behavior
HSM108	X	X	No Fix	Incorrect LBR Source Address May be Reported For a Transactional Abort
HSM109	X	X	No Fix	Address Translation Faults for Intel® VT-d May Not be Reported for Display Engine Memory Accesses
HSM110	X	X	No Fix	L3 Cache Corrected Error Count May be Inaccurate After Package C7 Exit
HSM111	X	X	No Fix	PCIe* Device's SVID is Not Preserved Across The Package C7 C-State
HSM112 ²	X	X	No Fix	Warm Reset Does Not Stop GT Power Draw
HSM113 ²	X	X	No Fix	Unused PCIe* Lanes May Remain Powered After Package C7
HSM114 ²	X	X	No Fix	BMI1 And BMI2 Instruction Groups Are Not Available
HSM115 ¹	X	X	No Fix	HD Audio Device Playback May Be Interrupted if The Processor Enters a Deep Package C-State
HSM116	X	X	No Fix	Virtual-APIC Page Accesses With 32-Bit PAE Paging May Cause a System Crash



Errata (Sheet 5 of 7)

Number	Steppings		Status	ERRATA
	C-0	D-0		
HSM117	X	X	No Fix	Processor Energy Policy Selection May Not Work as Expected
HSM118	X	X	No Fix	Processor May Not be Able to Reduce The Graphics Engine's Effective Frequency
HSM119	X	X	No Fix	A PEBS Record May Contain Processor State for an Unexpected Instruction
HSM120	X	X	No Fix	MSR_PP1_ENERGY_STATUS Reports Incorrect Energy Data
HSM121	X	X	No Fix	x87 FPU DP May be Incorrect After Instructions That Save FP State to Memory
HSM122	X	X	No Fix	Processor May Hang During Package C7 Exit
HSM123 ¹	X	X	No Fix	Certain Processors May Experience Transient LLC ECC Errors
HSM124	X	X	No Fix	N/A. Erratum has been removed
HSM125	X	X	No Fix	Spurious LLC Machine Check May Occur
HSM126	X	X	No Fix	Page Fault May Report Incorrect Fault Information
HSM127	X	X	No Fix	CATERR# Pin Assertion is Not Cleared on a Warm Reset
HSM128	X	X	No Fix	Uncorrectable Machine Check Error During Core C6 Entry May Not be Signaled
HSM129	X	X	No Fix	The SAMPLE/PRELOAD JTAG Command Does Not Sample The Display Transmit Signals
HSM130	X	X	No Fix	Performance Monitor Event For Outstanding Offcore Requests And Snoop Requests May be Incorrect
HSM131 ²	X	X	No Fix	Processor Energy Policy Selection May Not Work as Expected
HSM132 ²	X	X	No Fix	PCIe Link May Incorrectly Train to 8.0 GT/s
HSM133 ²	X	X	No Fix	PCIe Tx Voltage Reference Cannot be Changed
HSM134	X	X	No Fix	VM Exit May Set IA32_EFER.NXE When IA32_MISC_ENABLE Bit 34 is Set to 1
HSM135 ³	X	X	No Fix	Re-enabling eDRAM May Log a Machine Check and Hang
HSM136 ³	X	X	No Fix	Warm Reset Does Not Stop EDRAM Power Draw
HSM137	X	X	No Fix	CHAP Counter Values May be Cleared After Package C7 or Deeper C-State
HSM138	X	X	No Fix	Opcode Bytes F3 0F BC May Execute As TZCNT Even When TZCNT Not Enumerated by CPUID
HSM139	X	X	No Fix	Intel® S2DDT May Not Function Correctly with Certain High Resolution Displays
HSM140	X	X	No Fix	N/A. Errata has been Removed
HSM141	X	X	No Fix	VM Exit May Set IA32_EFER.NXE When IA32_MISC_ENABLE Bit 34 is Set to 1
HSM142	X	X	No Fix	Spurious Corrected Errors May be Reported
HSM143	X	X	No Fix	A MOV to CR3 When EPT is Enabled May Lead to an Unexpected Page Fault or an Incorrect Page Translation
HSM144	X	X	No Fix	Package C7 Power Consumption Has Been Observed to be Higher Than Package C6
HSM145	X	X	No Fix	A HyperThreading Enabled Processor May Exhibit Unpredictable Behavior During Power or Thermal Management Operations
HSM146	X	X	No Fix	Certain Perfmon Events May be Counted Incorrectly When The Processor is Not in C0 State



Errata (Sheet 6 of 7)

Number	Steppings		Status	ERRATA
	C-0	D-0		
HSM147 ¹	X	X	No Fix	System Hang May Occur During Exit From Package C7 Due to VccST sensitivity
HSM148	X	X	No Fix	Software Using Intel® TSX May Result in Unpredictable System Behavior
HSM149	X	X	No Fix	Running All Cores May Incorrectly Limit the Processor Frequency
HSM150	X	X	No Fix	Concurrent Core And Graphics Operation at Turbo Ratios May Lead to System Hang
HSM151	X	X	No Fix	Performance Monitor Instructions Retired Event May Not Count Consistently
HSM152 ³	X	X	No Fix	Some Configurations May Violate Embedded DRAM Refresh Requirements Leading to a System Hang
HSM153	X	X	No Fix	Interactions Between Multiple Unaligned Memory Accesses And Locked Instructions May Lead to a Machine Check
HSM154	X	X	No Fix	Fixed-Function Performance Counter May Over Count Instructions Retired by 32 When Intel® Hyper-Threading Technology is Enabled
HSM155	X	X	No Fix	Performance Monitor UOPS_EXECUTED Event May Be Inaccurate When Using Intel® Hyper-Threading Technology
HSM156	X	X	No Fix	Operand-Size Override Prefix Causes 64-bit Operand Form of MOVBE Instruction to Cause a #UD
HSM157	X	X	No Fix	POPCNT Instruction May Take Longer to Execute Than Expected
HSM158	X	X	No Fix	System May Hang or Video May be Distorted After Graphics RC6 Exit
HSM159	X	X	No Fix	Certain eDP* Displays May Not Function as Expected
HSM160	X	X	No Fix	Some OFFCORE_RESPONSE Performance Monitoring Events May Undercount
HSM161	X	X	No Fix	Certain Settings of VM-Execution Controls May Result in Incorrect Linear-Address Translations
HSM162	X	X	No Fix	An IRET Instruction That Results in a Task Switch Does Not Serialize The Processor
HSM163	X	X	No Fix	Attempting to Disable Turbo Mode May Cause a #GP
HSM164 ³	X	X	No Fix	Machine Check Threshold Based Error Status May be Set Incorrectly
HSM165	X	X	No Fix	PECI Frequency Limited to 1 MHz
HSM166	X	X	No Fix	VGATHERQPS That Loads an Element From The APIC-Access Page May Load Other Elements From Incorrect Addresses
HSM167	X	X	No Fix	MTF VM Exit on XBEGIN Instruction May Save State Incorrectly
HSM168	X	X	No Fix	Uncore Performance Monitoring Counters May be Disabled or Cleared After Package C7
HSM169	X	X	No Fix	PEBS Record May Be Generated After Being Disabled
HSM170	X	X	No Fix	PCIe* Ports Do Not Support DLL Link Active Reporting
HSM171	X	X	No Fix	PCIe* Link Speed Negotiation May Fail After Link is Re-enabled
HSM172	X	X	No Fix	MOVNTDQA From WC Memory May Pass Earlier Locked Instructions
HSM173	X	X	No Fix	Data Breakpoint Coincident With a Machine Check Exception May be Lost
HSM174	X	X	No Fix	A Corrected Internal Parity Error May Result in a System Hang
HSM175	X	X	No Fix	An APIC Timer Interrupt During Core C6 Entry May Be Lost
HSM176	X	X	No Fix	Internal Power State Transitions May Cause the Graphics Device to Hang



Errata (Sheet 7 of 7)

Number	Steppings		Status	ERRATA
	C-0	D-0		
HSM177	X	X	No Fix	PEBS EventingIP Field May Be Incorrect Under Certain Conditions
HSM178	X	X	No Fix	RF May be Incorrectly Set in The EFLAGS That is Saved on a Fault in PEBS or BTS
HSM179	X	X	No Fix	Some Memory Performance Monitoring Events May Produce Incorrect Results When Filtering on Either OS or USR Modes
HSM180	X	X	No Fix	An x87 Store Instruction Which Pends #PE While EPT is Enabled May Lead to an Unexpected Machine Check and/or Incorrect x87 State Information
HSM181	X	X	No Fix	Load Latency Performance Monitoring Facility May Stop Counting
HSM182	X	X	No Fix	Writing MSR_LASTBRANCH_x_FROM_IP May #GP When Intel® TSX is Not Supported
HSM183	X	X	No Fix	APIC Timer Interrupt May Not be Generated at The Correct Time In TSC-Deadline Mode
HSM184	X	X	No Fix	System May Hang Under Complex Conditions
HSM185	X	X	No Fix	Instruction Fetch May Cause Machine Check if Page Size Was Changed Without Invalidation
HSM186	X	X	No Fix	Performance Monitoring General Counter 2 May Have Invalid Value Written When TSX Is Enabled
HSM187	X	X	No Fix	PMU MSR_UNC_PERF_FIXED_CTR is Cleared After Pkg C7 or Deeper

Notes:

1. Applies to 4th Generation Intel® Core™ processor based on Mobile U-Processor and Y-Processor Lines only
2. Applies to 4th Generation Intel® Core™ processor based on Mobile M-Processor and H-Processor Lines only
3. Applies to 4th Generation Intel® Core™ processor based on Mobile H-Processor Line (BGA) with GT3 Graphics only



Specification Changes

Number	SPECIFICATION CHANGES
	TSX Instruction

Specification Clarifications

Number	SPECIFICATION CLARIFICATIONS
	None for this revision of this specification update.

Documentation Changes

Number	DOCUMENTATION CHANGES
HSM1	""



Identification Information

Component Identification using Programming Interface

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

Table 1. 4th Generation Intel® Core™ Processor based on Mobile M-Processor Line Component Identification

Reserved	Extended Family	Extended Model	Reserved	Processor Type	Family Code	Model Number	Stepping ID
31:28	27:20	19:16	15:14	13:12	11:8	7:4	3:0
	00000000b	0011b		00b	0110b	1100b	xxxxb

Table 2. 4th Generation Intel® Core™ Processor based on Mobile H-Processor Line Component Identification

Reserved	Extended Family	Extended Model	Reserved	Processor Type	Family Code	Model Number	Stepping ID
31:28	27:20	19:16	15:14	13:12	11:8	7:4	3:0
	00000000b	0100b		00b	0110b	0110b	xxxxb

Table 3. 4th Generation Intel® Core™ Processor based on Mobile U/Y-Processor Line Component Identification

Reserved	Extended Family	Extended Model	Reserved	Processor Type	Family Code	Model Number	Stepping ID
31:28	27:20	19:16	15:14	13:12	11:8	7:4	3:0
	00000000b	0100b		00b	0110b	0101b	xxxxb

Notes:

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 Intel386™, Intel486™, Pentium®, Pentium 4, 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. See the processor Identification table for the processor stepping ID number in the CPUID information.

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. Note that 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.

The processor can be identified by the following register contents.


Table 4. Processor Identification by Register Contents

Processor line	Stepping	Vendor ID1	Host Device ID2	Processor Graphics Device ID3	Revision ID4	CRID
M-Processor Series	C-0	8086h	0C04h	GT1 = 0406h GT2 = 0416h	06h	06h
H-Processor Series	C-0	8086h	0C04h	GT2=0416h	06h	06h
H-Processor Series (BGA) with GT3 Graphics	C-0	8086h	0D04h	GT3 = 0D26h	08h	08h
U-Processor Series	C-0	8086h	0A04h	GT1 = 0A06h GT2 = 0A16h GT3 = 0A26h	GT1 = 0Bh GT2 = 0Bh GT3 = 09h	GT1 = 0Bh GT2 = 0Bh GT3 = 09h
U-Processor Series	D-0	8086h	0A04h	GT1 = 0A06h GT2 = 0A16h GT3 = 0A26h	GT1 = 0Bh GT2 = 0Bh GT3 = 09h	GT1 = 0Bh GT2 = 0Bh GT3 = 09h
Y-Processor Series (SDP = 6W)	C-0	8086h	0A04h	GT2 = 0A16h	GT2 = 0Bh	GT2 = 0Bh
Y-Processor Series (SDP = 6W)	D-0	8086h	0A04h	GT2=0A16h	GT2 = 0Bh	GT2 = 0Bh
Y -Processor Series (SDP = 4.5W)	D-0	8086h	0A04h	GT1 = 0A06h GT2 = 0A16h	GT1 = 0Bh GT2 = 0Bh	GT1 = 0Bh GT2 = 0Bh

Notes:

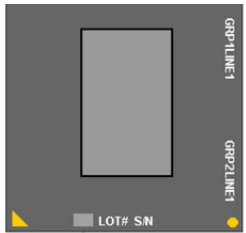
1. The Vendor ID corresponds to bits 15:0 of the Vendor ID Register located at offset 00h–01h in the PCI function 0 configuration space.
2. The Host Device ID corresponds to bits 15:0 of the Device ID Register located at Device 0 offset 02h–03h in the PCI function 0 configuration space.
3. The Processor Graphics Device ID (DID2) corresponds to bits 15:0 of the Device ID Register located at Device 2 offset 02h–03h in the PCI function 0 configuration space.
4. The Revision Number corresponds to bits 7:0 of the Revision ID Register located at offset 08h in the PCI function 0 configuration space.



Component Marking Information

The processor stepping can be identified by the following component markings.

Figure 1. Mobile 4th Generation Intel® Core™ Processor Family BGA Top-Side Markings



Pkg Size = 37.5mm x 32mm
Pin Count = 1364

Sample (QDF)
GRP1LINE1: i{M}{C}YY {FPO}QDF ES 22 max char/line, 16 pt font
GRP2LINE1: {e1} 2 max char/line, 29 pt font

Production (SSPEC)
GRP1LINE1: i{M}{C}YY {FPO} SSPEC 22 max char/line, 16 pt font
GRP2LINE1: {e1} 2 max char/line, 29 pt font

FOL Mark:
2D Matrix and Human Readable Lot# (9 characters) and Serial# (5 characters)

Table 5. 4th Generation Intel® Core™ Processor based on Mobile M-Processor and H-Processor Lines Processor Identification (Sheet 1 of 2)

S-Spec Number	Processor Number	Stepping	Cache Size (MB)	Functional Core	Integrated Graphics Cores	Max Turbo Freq. Rate (GHz)	Memory (MHz)	Core Freq. (GHz)	Thermal Design Power (W)
SR1VZ 1	i7-4700EC	C-0	8	4	N/A	N/A	1600	2.7	43
SR1W0 1	i7-4702EC	C-0	8	4	N/A	N/A	1600	2.0	27
SR1W1 1	i5-4402EC	C-0	4	2	N/A	N/A	1600	2.5	27
SR15E	i7-4700HQ	C-0	6	4	2	3.4	1600	2.4	47
SR15F	i7-4702HQ	C-0	6	4	2	3.2	1600	2.2	37
SR1BS	i7-4960HQ	C-0	6	4	2	3.8	1600	2.6	47
SR18G	i7-4950HQ	C-0	6	4	3	3.6	1600	2.4	47
SR18H	i7-4850HQ	C-0	6	4	3	3.5	1600	2.3	47
SR18J	i7-4750HQ	C-0	6	4	3	3.2	1600	2	47
SR15M	i7-4930MX	C-0	8	4	2	3.9	1600	3.000	57
SR15K	i7-4900MQ	C-0	8	4	2	3.8	1600	2.8	47
SR15L	i7-4800MQ	C-0	6	4	2	3.7	1600	2.7	47
SR15J	i7-4702MQ	C-0	6	4	2	3.2	1600	2.2	37
SR15H	i7-4700MQ	C-0	6	4	2	3.4	1600	2.4	47



Table 5. 4th Generation Intel® Core™ Processor based on Mobile M-Processor and H-Processor Lines Processor Identification (Sheet 2 of 2)

S-Spec Number	Processor Number	Stepping	Cache Size (MB)	Functional Core	Integrated Graphics Cores	Max Turbo Freq. Rate (GHz)	Memory (MHz)	Core Freq. (GHz)	Thermal Design Power (W)
SR1LF	Celeron 2970M	C-0	2	2	1	2.2	1600	2.2	37
SR1LC	Pentium 3560M	C-0	2	2	1	2.4	1600	2.4	37
SR1HB	i3-4100M	C-0	3	2	2	2.5	1600	2.5	37
SR1L7	i3-4110M	C-0	3	2	2	2.6	1600	2.6	37
SR1L4	i5-4210M	C-0	3	2	2	3.2	1600	2.6	37
SR1PX	i7-4710HQ	C-0	6	4	2	3.5	1600	2.5	47
SR1PQ	i7-4710MQ	C-0	6	4	2	3.5	1600	2.5	47
SR1PZ	i7-4712HQ	C-0	6	4	2	3.3	1600	2.3	37
SR1PS	i7-4712MQ	C-0	6	4	2	3.3	1600	2.3	37
SR1BM	i7-4760HQ	C-0	6	4	3	3.3	1600	2.1	47
SR1ZW	i7-4770HQ	C-0	6	4	3	3.4	1600	2.2	47
SR1ZX	i7-4870HQ	C-0	6	4	3	3.7	1600	2.5	47
SR1ZY	i7-4980HQ	C-0	6	4	3	4	1600	2.8	47
SR1Q0	i5-4210H	C-0	3	2	2	3.5	1600	2.9	47
SR17L 2	i7-4700EQ	C-0	6	4	2	3.4	1600	2.4	47
SR17M 2	i5-4400E	C-0	3	2	2	3.3	1600	2.7	37
SR1T1 2	i5-4422E	C-0	3	2	2	2.9	1600	1.8	25
SR1Q8	i7-4720HQ	C-0	6	4	2	3.6	1600	2.6	47
SR1PY	i7-4722HQ	C-0	6	4	2	3.4	1600	2.4	37

Note:

- These are based on 4th Generation Intel® Core™ processor Mobile H-Processor Line SKUs.
- These are based on 4th Generation Intel® Core™ processor Mobile M-Processor Line SKUs.

Table 6. 4th Generation Intel® Core™ Processor based on Mobile U-Processor and Y-Processor Lines Processor Identification (Sheet 1 of 3)

S-Spec Number	Processor Number	Stepping	Cache Size (MB)	Functional Core	Integrated Graphics Cores	Max Turbo Freq. Rate (GHz)	Memory (MHz)	Core Freq. (GHz)	Thermal Design Power (W)
SR16Z	i7-4500U	C-0	4	2	3	3	1600	1.8	15
SR16J	i7-4550U	C-0	4	2	3	3	1600	1.5	15
SR16H	i7-4650U	C-0	4	2	3	3.3	1600	1.7	15
SR16Y	Celeron 2955U	C-0	2	2	1	1.4	1600	1.4	15
SR1DM	Celeron 2980U	D-0	2	2	1	1.6	1600	1.6	15
SR1EK	i3-4005U	D-0	3	2	2	1.7	1600	1.7	15



Table 6. 4th Generation Intel® Core™ Processor based on Mobile U-Processor and Y-Processor Lines Processor Identification (Sheet 2 of 3)

S-Spec Number	Processor Number	Stepping	Cache Size (MB)	Functional Core	Integrated Graphics Cores	Max Turbo Freq. Rate (GHz)	Memory (MHz)	Core Freq. (GHz)	Thermal Design Power (W)
SR16Q	i3-4010U	C-0	3	2	2	1.7	1600	1.7	15
SR16P	i3-4100U	C-0	3	2	2	1.8	1600	1.8	15
SR170	i5-4200U	C-0	3	2	2	2.6	1600	1.6	15
SR16M	i5-4250U	C-0	3	2	3	2.6	1600	1.3	15
SR1ED	i5-4300U	D-0	3	2	2	2.9	1600	1.9	15
SR16L	i5-4350U	C-0	3	2	3	2.9	1600	1.4	15
SR1EA	i7-4600U	D-0	4	2	2	3.3	1600	2.1	15
SR1E3	Pentium 3556U	D-0	2	2	1	1.7	1600	1.7	15
SR1E0	Pentium 3665U	D-0	2	2	1	1.8	1600	1.8	15
SR1DE	Pentium 3560Y	D-0	2	2	1	1.2	1600	1.2	11.5
SR18F	i3-4010Y	C-0	3	2	2	1.3	1600	1.3	11.5
SR1DC	i3-4020Y	D-0	3	2	2	1.5	1600	1.5	11.5
SR18T	i5-4200Y	C-0	3	2	2	1.9	1600	1.4	11.5
SR191	i5-4210Y	D-0	3	2	2	1.9	1600	1.5	11.5
SR192	i5-4300Y	D-0	3	2	2	2.3	1600	1.6	11.5
SR18D	i7-4610Y	D-0	4	2	2	2.9	1600	1.7	11.5
SR190	i5-4202Y	D-0	3	2	2	2	1600	1.6	11.5
SR19B	i5-4302Y	D-0	3	2	2	2.3	1600	1.6	11.5
SR1C7	i3-4012Y	D-0	3	2	2	1.5	1600	1.5	11.5
SR188	i7-4558U	C-0	4	2	3	3.3	1600	2.8	28
SR189	i5-4288U	C-0	3	2	3	3.1	1600	2.6	28
SR18A	i5-4258U	C-0	3	2	3	2.9	1600	2.4	28
SR18B	i3-4158U	C-0	3	2	3	2	1600	2	28
SR1DG	Pentium 3561Y	D-0	2	2	1	1.2	1600	1.2	11.5
SR1E8	Pentium 3558U	D-0	2	2	1	1.7	1600	1.7	15
SR1DV	Celeron 2957U	D-0	2	2	1	1.4	1600	1.4	15
SR1DX	Celeron 2981U	D-0	2	2	1	1.6	1600	1.6	15
SR1EQ	i3-4025U	D-0	3	2	2	1.9	1600	1.9	15
SR1EN	i3-4030U	D-0	3	2	2	1.9	1600	1.9	15
SR1DD	i3-4030Y	D-0	3	2	2	1.6	1600	1.6	11.5
SR1EP	i3-4120U	D-0	3	2	2	2	1600	2	15
SR1EF	i5-4210U	D-0	3	2	2	2.7	1600	1.7	15



Table 6. 4th Generation Intel® Core™ Processor based on Mobile U-Processor and Y-Processor Lines Processor Identification (Sheet 3 of 3)

S-Spec Number	Processor Number	Stepping	Cache Size (MB)	Functional Core	Integrated Graphics Cores	Max Turbo Freq. Rate (GHz)	Memory (MHz)	Core Freq. (GHz)	Thermal Design Power (W)
SR1DB	I5-4220Y	D-0	3	2	2	2	1600	1.6	11.5
SR16T	I5-4260U	C-0	3	2	3	2.7	1600	1.4	15
SR1EB	I7-4510U	D-0	4	2	2	3.1	1600	2	15
SR1ZT	I7-4578U	C-0	4	2	3	3.5	1600	3	28
SR1ZU	I5-4308U	C-0	3	2	3	3.3	1600	2.8	28
SR1ZV	I5-4278U	C-0	3	2	3	3.1	1600	2.6	28

§ §



Errata

HSM1. LBR, BTS, BTM May Report a Wrong Address when an Exception/Interrupt Occurs in 64-bit Mode

Problem: An exception/interrupt event should be transparent to the LBR (Last Branch Record), BTS (Branch Trace Store) and BTM (Branch Trace Message) mechanisms. However, during a specific boundary condition where the exception/interrupt occurs right after the execution of an instruction at the lower canonical boundary (0x00007FFFFFFFFF) in 64-bit mode, the LBR return registers will save a wrong return address with bits 63 to 48 incorrectly sign extended to all 1's. Subsequent BTS and BTM operations which report the LBR will also be incorrect.

Implication: LBR, BTS and BTM may report incorrect information in the event of an exception/interrupt.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM2. EFLAGS Discrepancy on Page Faults and on EPT-Induced VM Exits after a Translation Change

Problem: This erratum is regarding the case where paging structures are modified to change a linear address from writable to non-writable without software performing an appropriate TLB invalidation. When a subsequent access to that address by a specific instruction (ADD, AND, BTC, BTR, BTS, CMPXCHG, DEC, INC, NEG, NOT, OR, ROL/ROR, SAL/SAR/SHL/SHR, SHLD, SHRD, SUB, XOR, and XADD) causes a page fault or an EPT-induced VM exit, the value saved for EFLAGS may incorrectly contain the arithmetic flag values that the EFLAGS register would have held had the instruction completed without fault or VM exit. For page faults, this can occur even if the fault causes a VM exit or if its delivery causes a nested fault.

Implication: None identified. Although the EFLAGS value saved by an affected event (a page fault or an EPT-induced VM exit) may contain incorrect arithmetic flag values, Intel has not identified software that is affected by this erratum. This erratum will have no further effects once the original instruction is restarted because the instruction will produce the same results as if it had initially completed without fault or VM exit.

Workaround: If the handler of the affected events inspects the arithmetic portion of the saved EFLAGS value, then system software should perform a synchronized paging structure modification and TLB invalidation.

Status: For the steppings affected, see the *Summary Table of Changes*.

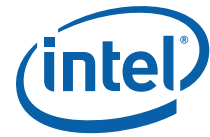
HSM3. MCI_Status Overflow Bit May Be Incorrectly Set on a Single Instance of a DTLB Error

Problem: A single Data Translation Look Aside Buffer (DTLB) error can incorrectly set the Overflow (bit [62]) in the MCI_Status register. A DTLB error is indicated by MCA error code (bits [15:0]) appearing as binary value, 000x 0000 0001 0100, in the MCI_Status register.

Implication: Due to this erratum, the Overflow bit in the MCI_Status register may not be an accurate indication of multiple occurrences of DTLB errors. There is no other impact to normal processor functionality.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM4. LER MSRs May Be Unreliable**

Problem: Due to certain internal processor events, updates to the LER (Last Exception Record) MSRs, MSR_LER_FROM_LIP (1DDH) and MSR_LER_TO_LIP (1DEH), may happen when no update was expected.

Implication: The values of the LER MSRs may be unreliable.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM5. MONITOR or CLFLUSH on the Local xAPIC's Address Space Results in Hang

Problem: If the target linear address range for a MONITOR or CLFLUSH is mapped to the local xAPIC's address space, the processor will hang.

Implication: When this erratum occurs, the processor will hang. The local xAPIC's address space must be uncached. The MONITOR instruction only functions correctly if the specified linear address range is of the type write-back. CLFLUSH flushes data from the cache. Intel has not observed this erratum with any commercially available software.

Workaround: Do not execute MONITOR or CLFLUSH instructions on the local xAPIC address space.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM6. An Uncorrectable Error Logged in IA32_CR_MC2_STATUS May also Result in a System Hang

Problem: Uncorrectable errors logged in IA32_CR_MC2_STATUS MSR (409H) may also result in a system hang causing an Internal Timer Error (MCACOD = 0x0400h) to be logged in another machine check bank (IA32_MCI_STATUS).

Implication: Uncorrectable errors logged in IA32_CR_MC2_STATUS can further cause a system hang and an Internal Timer Error to be logged.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM7. #GP on Segment Selector Descriptor that Straddles Canonical Boundary May Not Provide Correct Exception Error Code

Problem: During a #GP (General Protection Exception), 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, see the *Summary Table of Changes*.

**HSM8. FREEZE_WHILE_SMM Does Not Prevent Event From Pending PEBS During SMM**

Problem: In general, a PEBS record should be generated on the first count of the event after the counter has overflowed. However, IA32_DEBUGCTL_MSR.FREEZE_WHILE_SMM (MSR 1D9H, bit [14]) prevents performance counters from counting during SMM (System Management Mode). Due to this erratum, if:

1. A performance counter overflowed before an SMI.
2. A PEBS record has not yet been generated because another count of the event has not occurred.
3. The monitored event occurs during SMM then a PEBS record will be saved after the next RSM instruction.

When FREEZE_WHILE_SMM is set, a PEBS should not be generated until the event occurs outside of SMM.

Implication: A PEBS record may be saved after an RSM instruction due to the associated performance counter detecting the monitored event during SMM; even when FREEZE_WHILE_SMM is set.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM9. APIC Error “Received Illegal Vector” May be Lost

Problem: APIC (Advanced Programmable Interrupt Controller) may not update the ESR (Error Status Register) flag Received Illegal Vector bit [6] properly when an illegal vector error is received on the same internal clock that the ESR is being written (as part of the write-read ESR access flow). The corresponding error interrupt will also not be generated for this case.

Implication: Due to this erratum, an incoming illegal vector error may not be logged into ESR properly and may not generate an error interrupt.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

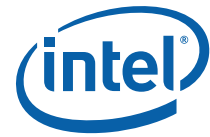
HSM10. Changing the Memory Type for an In-Use Page Translation May Lead to Memory-Ordering Violations

Problem: Under complex microarchitectural conditions, if software changes the memory type for data being actively used and shared by multiple threads without the use of semaphores or barriers, software may see load operations execute out of order.

Implication: Memory ordering may be violated. Intel has not observed this erratum with any commercially available software.

Workaround: Software should ensure pages are not being actively used before requesting their memory type be changed.

Status: For the steppings affected, see the *Summary Table of Changes*.



HSM11. Performance Monitor Precise Instruction Retired Event May Present Wrong Indications

Problem: When the PDIR (Precise Distribution for Instructions Retired) mechanism is activated (INST_RETIRE.ALL (event C0H, umask value 00H) on Counter 1 programmed in PEBS mode), the processor may return wrong PEBS/PMI interrupts and/or incorrect counter values if the counter is reset with a SAV below 100 (Sample-After-Value is the counter reset value software programs in MSR IA32_PMC1[47:0] in order to control interrupt frequency).

Implication: Due to this erratum, when using low SAV values, the program may get incorrect PEBS or PMI interrupts and/or an invalid counter state.

Workaround: The sampling driver should avoid using SAV<100.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM12. CR0.CD Is Ignored in VMX Operation

Problem: If CR0.CD=1, the MTRRs and PAT should be ignored and the UC memory type should be used for all memory accesses. Due to this erratum, a logical processor in VMX operation will operate as if CR0.CD=0 even if that bit is set to 1.

Implication: Algorithms that rely on cache disabling may not function properly in VMX operation.

Workaround: Algorithms that rely on cache disabling should not be executed in VMX root operation.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM13. N/A. Erratum has been removed

HSM14. 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, see the *Summary Table of Changes*.

HSM15. Processor May Fail to Acknowledge a TLP Request

Problem: When a PCIe root port's receiver is in Receiver L0s power state and the port initiates a Recovery event, it will issue Training Sets to the link partner. The link partner will respond by initiating an L0s exit sequence. Prior to transmitting its own Training Sets, the link partner may transmit a TLP (Transaction Layer Packet) request. Due to this erratum, the root port may not acknowledge the TLP request.

Implication: After completing the Recovery event, the PCIe link partner will replay the TLP request. The link partner may set a Correctable Error status bit, which has no functional effect.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM16. Interrupt From Local APIC Timer May Not Be Detectable While Being Delivered**

Problem: If the local-APIC timer's CCR (current-count register) is 0, software should be able to determine whether a previously generated timer interrupt is being delivered by first reading the delivery-status bit in the LVT timer register and then reading the bit in the IRR (interrupt-request register) corresponding to the vector in the LVT timer register. If both values are read as 0, no timer interrupt should be in the process of being delivered. Due to this erratum, a timer interrupt may be delivered even if the CCR is 0 and the LVT and IRR bits are read as 0. This can occur only if the DCR (Divide Configuration Register) is greater than or equal to 4. The erratum does not occur if software writes zero to the Initial Count Register before reading the LVT and IRR bits.

Implication: Software that relies on reads of the LVT and IRR bits to determine whether a timer interrupt is being delivered may not operate properly.

Workaround: Software that uses the local-APIC timer must be prepared to handle the timer interrupts, even those that would not be expected based on reading CCR and the LVT and IRR bits; alternatively, software can avoid the problem by writing zero to the Initial Count Register before reading the LVT and IRR bits.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM17. PCIe* Root-port Initiated Compliance State Transmitter Equalization Settings May be Incorrect

Problem: If the processor is directed to enter PCIe Polling.Compliance at 5.0 GT/s or 8.0 GT/s transfer rates, it should use the Link Control 2 Compliance Preset/De-emphasis field (bits [15:12]) to determine the correct de-emphasis level. Due to this erratum, when the processor is directed to enter Polling.Compliance from 2.5 GT/s transfer rate, it retains 2.5 GT/s de-emphasis values.

Implication: The processor may operate in Polling.Compliance mode with an incorrect transmitter de-emphasis level.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

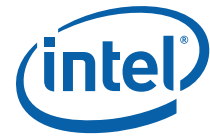
HSM18. PCIe* Controller May Incorrectly Log Errors on Transition to RxL0s

Problem: Due to this erratum, if a link partner transitions to RxL0s state within 20 ns of entering L0 state, the PCIe controller may incorrectly log an error in "Correctable Error Status.Receiver Error Status" field (Bus 0, Device 2, Function 0, 1, 2 and Device 6, Function 0, offset 1D0H, bit 0).

Implication: Correctable receiver errors may be incorrectly logged. Intel has not observed any functional impact due to this erratum with any commercially available add-in cards.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM19. Unused PCIe* Lanes May Report Correctable Errors**

Problem: Due to this erratum, during PCIe* link down configuration, unused lanes may report a Correctable Error Detected in Bus 0, Device 1, Function 0-2, and Device 6, Function 0, Offset 158H, Bit 0.

Implication: Correctable Errors may be reported by a PCIe controller for unused lanes.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM20. Accessing Physical Memory Space 0-640K through the Graphics Aperture May Cause Unpredictable System Behavior

Problem: The physical memory space 0-640K when accessed through the graphics aperture may result in a failure for writes to complete or reads to return incorrect results.

Implication: A hang or functional failure may occur during graphics operation such as OGL or OCL conformance tests, 2D/3D games and graphics-intensive application.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM21. PCIe Root Port May Not Initiate Link Speed Change

Problem: The PCIe Base specification requires the upstream component to maintain the PCIe link at the target link speed or the highest speed supported by both components on the link, whichever is lower. PCIe root port will not initiate the link speed change without being triggered by the software when the root port maximum link speed is configured to be 5.0 GT/s. System BIOS will trigger the link speed change under normal boot scenarios. However, BIOS is not involved in some scenarios such as link disable/re-enable or secondary bus reset and therefore the speed change may not occur unless initiated by the downstream component. This erratum does not affect the ability of the downstream component to initiate a link speed change. All known 5.0Gb/s-capable PCIe downstream components have been observed to initiate the link speed change without relying on the root port to do so.

Implication: Due to this erratum, the PCIe root port may not initiate a link speed change during some hardware scenarios causing the PCIe link to operate at a lower than expected speed. Intel has not observed this erratum with any commercially available platform.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM22. Pending x87 FPU Exceptions (#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 executed while Enhanced Intel SpeedStep® Technology transitions, Intel® Turbo Boost Technology transitions, or Thermal Monitor events occur, the pending #MF may be signaled 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, see the *Summary Table of Changes*.

**HSM23. DR6.B0-B3 May Not Report All Breakpoints Matched When a MOV/POP SS is Followed by a Store or an MMX Instruction**

Problem: Normally, data breakpoints match that occur on a MOV SS, r/m or POP SS will not cause a debug exception immediately after MOV/POP SS but will be delayed until the instruction boundary following the next instruction is reached. After the debug exception occurs, DR6.B0-B3 bits will contain information about data breakpoints matched during the MOV/POP SS as well as breakpoints detected by the following instruction. Due to this erratum, DR6.B0-B3 bits may not contain information about data breakpoints matched during the MOV/POP SS when the following instruction is either an MMX instruction that uses a memory addressing mode with an index or a store instruction.

Implication: When this erratum occurs, DR6 may not contain information about all breakpoints matched. This erratum will not be observed under the recommended usage of the MOV SS,r/m or POP SS instructions (i.e., following them only with an instruction that writes (E/R)SP).

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM24. VEX.L is Not Ignored with VCVT*2SI Instructions

Problem: The VEX.L bit should be ignored for the VCVTSS2SI, VCVTSD2SI, VCVTTSS2SI, and VCVTTSD2SI instructions, however due to this erratum the VEX.L bit is not ignored and will cause a #UD.

Implication: Unexpected #UDs will be seen when the VEX.L bit is set to 1 with VCVTSS2SI, VCVTSD2SI, VCVTTSS2SI, and VCVTTSD2SI instructions.

Workaround: Software should ensure that the VEX.L bit is set to 0 for all scalar instructions.

Status: For the steppings affected, see the *Summary Table of Changes*.

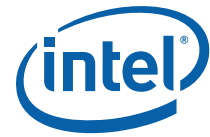
HSM25. Processor May Shut Down During Boundary Scan Testing

Problem: If the HIGHZ TAP command is run before initializing the Boundary Scan chain, the VR_EN pin may be tristated. The VR_EN pin may also be tristated by the EXTEST TAP command. The VR_EN signal controls the external voltage regulator; tristating VR_EN may disable the voltage regulator.

Implication: Due to this erratum, the processor may shut down.

Workaround: Initialize the Boundary Scan chain by running the PRELOAD TAP command before running HIGHZ TAP command or EXTEST TAP command.

Status: For the steppings affected, see the *Summary Table of Changes*.



HSM26. Some DRAM and L3 Cache Performance Monitoring Events May Count Incorrectly

Problem: Due to this erratum, the supplier information may become stale, and the following events may count incorrectly.

MEM_LOAD_UOPS_RETIRE.L3_HIT (Event D1H Umask 04H)

MEM_LOAD_UOPS_RETIRE.L3_MISS (Event D1H Umask 20H)

MEM_LOAD_UOPS_L3_HIT_RETIRE.XSNP_MISS (Event D2H Umask 01H)

MEM_LOAD_UOPS_L3_HIT_RETIRE.XSNP_HIT (Event D2H Umask 02H)

MEM_LOAD_UOPS_L3_HIT_RETIRE.XSNP_HITM (Event D2H Umask 04H)

MEM_LOAD_UOPS_L3_HIT_RETIRE.XSNP_NONE (Event D2H Umask 08H)

MEM_LOAD_UOPS_L3_MISS_RETIRE.LOCAL_DRAM (Event D3H Umask 01H)

MEM_TRANS_RETIRE.LOAD_LATENCY (Event CDH Umask 01H)

PAGE_WALKER_LOADS.DTLB_L3 (Event BCH Umask 14H)

PAGE_WALKER_LOADS.ITLB_L3 (Event BCH Umask 24H)

PAGE_WALKER_LOADS.DTLB_Memory (Event BCH Umask 18H)

PAGE_WALKER_LOADS.ITLB_Memory (Event BCH Umask 28H)

Implication: The affected events may count incorrectly, resulting in inaccurate memory profiles. For the affected events that are precise, PEBS records may be generated at incorrect points. Intel has observed incorrect counts by as much as 40%.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM27. Specific Graphics Blitter Instructions May Result in Unpredictable Graphics Controller Behavior

Problem: Specific source-copy blitter instructions in Intel® HD Graphics 4600 Processor may result in unpredictable behavior when a blit source and destination overlap.

Implication: Due to this erratum, the processor may exhibit unpredictable graphics controller behavior. Intel has not observed this erratum with any commercially available software.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM28. Processor May Enter Shutdown Unexpectedly on a Second Uncorrectable Error

Problem: If an IA32_MCI_STATUS MSR contains an uncorrectable error with MCACOD=0x406 and a second uncorrectable error occurs after warm reset but before the first error is cleared by zeroing the IA32_MCI_STATUS MSR, a shutdown will occur.

Implication: When this erratum occurs, the processor will unexpectedly shut down instead of executing the machine check handler.

Workaround: None identified. Software should clear IA32_MCI_STATUS MSRs as early as possible to minimize the possibility of this erratum occurring.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM29. Modified Compliance Patterns for 2.5 GT/s and 5 GT/s Transfer Rates Do Not Follow PCIe* Specification**

Problem: The PCIe controller does not produce the PCIe specification defined sequence for the Modified Compliance Pattern at 2.5 GT/s and 5 GT/s transfer rates. This erratum is not seen at 8 GT/s transfer rates.

Implication: Normal PCIe operation is unaffected by this erratum.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM30. Performance Monitor Counters May Produce Incorrect Results

Problem: When operating with SMT enabled, a memory at-retirement performance monitoring event (from the list below) may be dropped or may increment an enabled event on the corresponding counter with the same number on the physical core's other thread rather than the thread experiencing the event. Processors with SMT disabled in BIOS are not affected by this erratum.

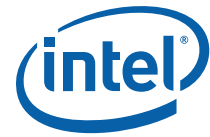
The list of affected memory at-retirement events is as follows:

MEM_UOP_RETIREDD.LOADS
MEM_UOP_RETIREDD.STORES
MEM_UOP_RETIREDD.LOCK
MEM_UOP_RETIREDD.SPLIT
MEM_UOP_RETIREDD.STLB_MISS
MEM_LOAD_UOPS_RETIREDD.HIT_LFB
MEM_LOAD_UOPS_RETIREDD.L1_HIT
MEM_LOAD_UOPS_RETIREDD.L2_HIT
MEM_LOAD_UOPS_RETIREDD.L3_HIT
MEM_LOAD_UOPS_L3_HIT_RETIREDD.XSNP_HIT
MEM_LOAD_UOPS_L3_HIT_RETIREDD.XSNP_HITM
MEM_LOAD_UOPS_L3_HIT_RETIREDD.XSNP_MISS
MEM_LOAD_UOPS_L3_HIT_RETIREDD.XSNP_NONE
MEM_LOAD_UOPS_RETIREDD.L3_MISS
MEM_LOAD_UOPS_L3_MISS_RETIREDD.LOCAL_DRAM
MEM_LOAD_UOPS_L3_MISS_RETIREDD.REMOTE_DRAM
MEM_LOAD_UOPS_RETIREDD.L2_MISS

Implication: Due to this erratum, certain performance monitoring event will produce unreliable results during hyper-threaded operation.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.



HSM31. Performance Monitor UOPS_EXECUTED Event May Undercount

Problem: The performance monitor event UOPS_EXECUTED (Event B1H, any Unmask) should count the number of UOPs executed each cycle. However due to this erratum, when eight UOPs execute in one cycle, these UOPs will not be counted.

Implication: The performance monitor event UOPS_EXECUTED may reflect a count lower than the actual number of events.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM32. MSR_PERF_STATUS May Report an Incorrect Core Voltage

Problem: The core operating voltage can be determined by dividing MSR_PERF_STATUS MSR (198H) bits [47:32] by 2^{13} . However, due to this erratum, this calculation may report half the actual core voltage.

Implication: The core operating voltage may be reported incorrectly.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM33. PCIe* Atomic Transactions From Two or More PCIe Controllers May Cause Starvation

Problem: On a Processor PCIe controller configuration in which two or more controllers receive concurrent atomic transactions, a PCIe controller may experience starvation which eventually can lead to a completion timeout.

Implication: Atomic transactions from two or more PCIe controllers may lead to a completion timeout. Atomic transactions from only one controller will not be affected by this erratum. Intel has not observed this erratum with any commercially available device.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM34. The Corrected Error Count Overflow Bit in IA32_MC0_STATUS is Not Updated When The UC Bit is Set

Problem: After a UC (uncorrected) error is logged in the IA32_MC0_STATUS MSR (401H), corrected errors will continue to be counted in the lower 14 bits (bits 51:38) of the Corrected Error Count. Due to this erratum, the sticky count overflow bit (bit 52) of the Corrected Error Count will not get updated when the UC bit (bit 61) is set to 1.

Implication: The Corrected Error Count Overflow indication will be lost if the overflow occurs after an uncorrectable error has been logged.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM35. An AVX Gather Instruction That Causes an EPT Violation May Not Update Previous Elements

Problem: When execution of an AVX gathers instruction causes an EPT (extended page table) violation due to a specific element, all previous elements should be complete. Due to this erratum, such an execution may fail to complete previous elements. In addition, the instruction's mask operand is not updated. This erratum applies only if the EPT violation occurs while updating an accessed or dirty flag in a paging-structure entry. Instructions impacted by this erratum are: VGATHERDPS, VGATHERDPD, VGATHERQPS, VGATHERQPD, VPGATHERDD, VPGATHERDQ, VPGATHERQD, and VPGATHERQQ.



Implication: This erratum may prevent a gather instruction from making forward progress.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM36. PLATFORM_POWER_LIMIT MSR Not Visible

Problem: The PLATFORM_POWER_LIMIT MSR (615H) is used to control the PL3 (power limit 3) mechanism of the processor. Due to this erratum, this MSR is not visible to software.

Implication: Software is unable to read or write the PLATFORM_POWER_LIMIT MSR. If software attempts to access this MSR, a general protection fault will occur.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM37. LPDDR Memory May Report Incorrect Temperature

Problem: When any of the four possible LPDDR ranks are not populated, the unpopulated ranks will report a default temperature of 85C as a three-bit value of 011b. If the system has unpopulated ranks the temperature of memory will be reported as 85C in PCU_CR_DDR_DIMM_HOTTEST_ABSOLUTE (MCHBAR Bus 0; Device 0; Function 0; offset 58B8H) in bits [5:7], until any of the populated ranks report a higher temperature than this.

Implication: When the memory temperature is less than or equal to 85C it may be reported as 85C. This erratum does not affect DDR3 and DDR3L memory types.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM38. PCIe* Host Bridge DID May Be Incorrect

Problem: The PCIe Host Bridge DID register (Bus 0; Device 0; Offset 2H) contents may be incorrect after a Package C7 exit.

Implication: Software that depends on the Host Bridge DID value may not behave as expected after a Package C7 exit.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM39. TSC May be Incorrect After a Deep C-State Exit

Problem: On exiting from Package C6 or deeper, the processor may incorrectly restore the TSC (Time Stamp Counter).

Implication: Software using the TSC may produce incorrect result and/or may not behave as expected.-

Workaround: It is possible for BIOS to contain a workaround for this erratum.

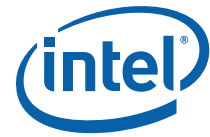
Status: For the steppings affected, see the *Summary Table of Changes*.

HSM40. PCIe* Controller May Initiate Speed Change While in DL_Init State Causing Certain PCIe Devices to Fail to Train

Problem: The PCIe controller supports hardware autonomous speed change capabilities. Due to this erratum, the PCIe controller may initiate speed change while in the DL_Init state which may prevent link training for certain PCIe devices.

Implication: Certain PCIe devices may fail to complete DL_Init causing the PCIe link to fail to train.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.



Status: For the steppings affected, see the *Summary Table of Changes*.

HSM41. Spurious VT-d Interrupts May Occur When the PFO Bit is Set

Problem: When the PFO (Primary Fault Overflow) field (bit [0] in the VT-d FSTS [Fault Status] register) is set to 1, further faults should not generate an interrupt. Due to this erratum, further interrupts may still occur.

Implication: Unexpected Invalidation Queue Error interrupts may occur. Intel has not observed this erratum with any commercially available software.

Workaround: Software should be written to handle spurious VT-d fault interrupts.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM42. N/A. Erratum has been removed

HSM43. AVX Gather Instruction That Causes a Fault or VM Exit May Incorrectly Modify Its Destination Register

Problem: An execution of a 128-bit AVX gather instruction zeroes the upper 128 bits of the instruction's destination register unless access to the first unmasked element causes a fault or VM exit. Due to this erratum, these bits may be cleared even when accessing the first unmasked element causes a fault or VM exit. Instructions impacted by this erratum are: VGATHERDPS, VGATHERDPD, VGATHERQPS, VGATHERQPD, VPGATHERDD, VPGATHERDQ, VPGATHERQD, and VPGATHERQQ.

Implication: Software that depends on the destination register of a 128-bit AVX gather instruction to remain unchanged after access of the first unmasked element results in fault or VM exit may not behave as expected.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM44. Inconsistent NaN Propagation May Occur When Executing (V)DPPS Instruction

Problem: Upon completion of the (V)DPPS instruction with multiple different NaN encodings in the input elements, software may observe different NaN encodings in the destination elements.

Implication: Inconsistent NaN encodings in the destination elements for the (V) DPPS instruction may be observed.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM45. Display May Flicker When Package C-States Are Enabled

Problem: When package C-States are enabled, the display may not be refreshed at the correct rate.

Implication: When this erratum occurs, the user may observe flickering on the display.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM46. Certain Combinations of AVX Instructions May Cause Unpredictable System Behavior**

Problem: Execution of certain combinations of AVX instructions may lead to unpredictable system behavior.

Implication: When this erratum occurs, unpredictable system behaviors, including system hang or incorrect results can occur.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM47. Processor May Incorrectly Estimate Peak Power Delivery Requirements

Problem: Under certain conditions, the processor may incorrectly calculate the frequency at which the cores and graphics engine can operate while still meeting voltage regulator and power supply peak power delivery capabilities. When this occurs, combined with high power workloads, system shutdown may be observed.

Implication: When this erratum occurs, system shutdown may be observed under high power workloads.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM48. IA32_PERF_CTL MSR is Incorrectly Reset

Problem: The IA32_PERF_CTL MSR (199H) is not initialized correctly after a processor reset.

Implication: If software reads the IA32_PERF_CTL MSR before writing it, software can observe an incorrect reset value. Although incorrect values are reported to software, the correct default values for this register are still used by the processor. No performance or power impact occurs due to this erratum.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM49. Processor May Hang During a Function Level Reset of the Display

Problem: When package C-States are enabled, it is possible that the processor may hang when software performs a Function Level Reset of the display via bit 1 of the Advanced Features Control Register (Bus 0; Device 2; Function 0; Offset 0A8H).

Implication: When this erratum occurs, the processor may hang.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

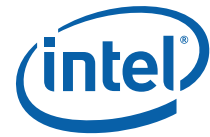
HSM50. AVX Gather Instruction That Should Result in #DF May Cause Unexpected System Behavior

Problem: Due to this erratum, an execution of a 128-bit AVX gather instruction may fail to generate a #DF (double fault) when expected. Instructions impacted by this erratum are: VGATHERDPS, VGATHERDPD, VGATHERQPS, VGATHERQPD, VPGATHERDD, VPGATHERDQ, VPGATHERQD, and VPGATHERQQ.

Implication: When this erratum occurs, an operation which should cause a #DF may result in unexpected system behavior.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.



HSM51. Throttling and Refresh Rate Maybe be Incorrect After Exiting Package C-State

- Problem:** When the OLTM (Open Loop Thermal Management) feature is enabled, the DIMM thermal status reported in DDR_THERM_PERDIMM_STATUS (MCHBAR Offset 588CH) may be incorrect following an exit from Package C3 or deeper.
- Implication:** The incorrect DIMM thermal status may result in degraded performance from unneeded memory throttling and excessive DIMM refresh rates.
- Workaround:** It is possible for BIOS to contain a workaround for this erratum.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

HSM52. Processor May Livelock During On Demand Clock Modulation

- Problem:** The processor may livelock when (1) a processor thread has enabled on demand clock modulation via bit 4 of the IA32_CLOCK_MODULATION MSR (19AH) and the clock modulation duty cycle is set to 12.5% (02H in bits 3:0 of the same MSR), and (2) the other processor thread does not have on demand clock modulation enabled and that thread is executing a stream of instructions with the lock prefix that either split a cacheline or access UC memory.
- Implication:** Program execution may stall on both threads of the core subject to this erratum.
- Workaround:** This erratum will not occur if clock modulation is enabled on all threads when using on demand clock modulation **or if** the duty cycle programmed in the IA32_CLOCK_MODULATION MSR is 18.75% or higher.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

HSM53. IA32_DEBUGCTL.FREEZE_PERFMON_ON_PMI is Incorrectly Cleared by SMI

- Problem:** FREEZE_PERFMON_ON_PMI (bit 12) in the IA32_DEBUGCTL MSR (1D9H) is erroneously cleared during delivery of an SMI (system-management interrupt).
- Implication:** As a result of this erratum, the performance monitoring counters will continue to count after a PMI occurs in SMM (system-management Mode).
- Workaround:** None identified.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

HSM54. The From-IP for Branch Tracing May be Incorrect

- Problem:** BTM (Branch Trace Message) and BTS (Branch Trace Store) report the "From-IP" indicating the source address of the branch instruction. Due to this erratum, BTM and BTS may repeat the "From-IP" value previously reported. The "To-IP" value is not affected.
- Implication:** Using BTM or BTS reports to reconstruct program execution may be unreliable.
- Workaround:** It is possible for the BIOS to contain a workaround for this erratum.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

HSM55. TM1 Throttling May Continue indefinitely

- Problem:** TM1 (Thermal Monitor 1) throttling may continue when the processor's temperature decreases below the throttling point while the processor is in Package C3 or deeper.
- Implication:** The processor will continue thermal throttling but does not indicate it is hot.
- Workaround:** It is possible for the BIOS to contain a workaround for this erratum.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

**HSM56. Internal Parity Errors May Incorrectly Report Overflow in The IA32_MC2_STATUS MSR**

Problem: Due to this erratum, uncorrectable internal parity error with an IA32_MC2_STATUS.MCACOD (bits [15:0]) value of 0005H and an IA32_MC2_STATUS.MSCOD (bits [31:16]) value of 0004H may incorrectly set the IA32_MC2_STATUS.OVER flag (bit 62) indicating an overflow when a single error has been observed.

Implication: IA32_MC2_STATUS.OVER may not accurately indicate multiple occurrences of uncorrectable internal parity errors. There is no other impact to normal processor functionality.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM57. Performance Monitor Events OTHER_ASSISTS.AVX_TO_SSE And OTHER_ASSISTS.SSE_TO_AVX May Over Count

Problem: The Performance Monitor events OTHER_ASSISTS.AVX_TO_SSE (Event C1H; Umask 08H) and OTHER_ASSISTS.SSE_TO_AVX (Event C1H; Umask 10H) incorrectly increment and over count when an HLE (Hardware Lock Elision) abort occurs.

Implication: The Performance Monitor Events OTHER_ASSISTS.AVX_TO_SSE And OTHER_ASSISTS.SSE_TO_AVX may over count.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM58. Processor May Run at Incorrect P-State

Problem: The processor package may use stale software P-State (performance state) requests when one or more logical processors are idle.

Implication: The processor package may run at a higher or lower than expected P-State. This issue may persist as long as any logical processor is idle.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM59. Performance Monitor Event DSB2MITE_SWITCHES.COUNT May Over Count

Problem: The Performance Monitor Event DSB2MITE_SWITCHES.COUNT (Event ABH; Umask 01H) should count the number of DSB (Decode Stream Buffer) to MITE (Macro Instruction Translation Engine) switches. Due to this erratum, the DSB2MITE_SWITCHES.COUNT event will count speculative switches and cause the count to be higher than expected.

Implication: The Performance Monitor Event DSB2MITE_SWITCHES.COUNT may report count higher than expected.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM60. Performance Monitor Register UNC_PERF_GLOBAL_STATUS Not Restored on Package C7 Exit**

Problem: MSR_UNC_PERF_GLOBAL_STATUS (392H) is a global status register which indicates the overflow of uncore performance monitor counters. The content of this register is lost in package C7 state.

Implication: If any uncore performance monitor counter has overflowed before entering the package C7 state, the MSR_UNC_PERF_GLOBAL_STATUS register will no longer reflect the overflow after exiting C7 state.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM61. Processor May Not Enter Package C6 or Deeper C-states When PCIe* Links Are Disabled

Problem: If the PCIe links are disabled via Link Disable (Bus 0, Device 1, Functions [2:1], Offset B0h, bit 4) and the PCIe controller is enabled (Bus 0, Device 0, Function 0, Offset 54h, bits [2:1] = '11), then the processor will be unable to enter Package C6 or deeper C-states.

Implication: Due to this erratum, the process will not enter Package C6 or deeper C-states.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM62. Performance Monitor Event For Outstanding Offcore Requests And Snoop Requests May Over Count

Problem: The performance monitor event OFFCORE_REQUESTS_OUTSTANDING (Event 60H, any Umask Value) should count the number of offcore outstanding transactions each cycle. Due to this erratum, the counts may be higher than actual number of events.

Implication: The performance monitor events OFFCORE_REQUESTS_OUTSTANDING may reflect counts higher than the actual number of events.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM63. Some Performance Monitor Event Counts May be Inaccurate During SMT Mode

Problem: The performance monitor event OFFCORE_REQUESTS_OUTSTANDING (Event 60H, any Umask Value) should count the number of occurrences that loads or stores stay in the super queue each cycle. The performance monitor event CYCLE_ACTIVITY.CYCLES_L2_PENDING (Event A3H, Umask 01H) should count the number of cycles that demand loads stay in the super queue. However, due to this erratum, these events may count inaccurately during SMT mode.

Implication: The performance monitor events OFFCORE_REQUESTS_OUTSTANDING and CYCLE_ACTIVITY.L2_PENDING may be unreliable during SMT Mode.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM64. N/A. Errata has been Removed****HSM65. The Upper 32 Bits of CR3 May be Incorrectly Used With 32-Bit Paging**

Problem: When 32-bit paging is in use, the processor should use a page directory located at the 32-bit physical address specified in bits 31:12 of CR3; the upper 32 bits of CR3 should be ignored. Due to this erratum, the processor will use a page directory located at the 64-bit physical address specified in bits 63:12 of CR3.

Implication: The processor may use an unexpected page directory or, if EPT (Extended Page Tables) is in use, cause an unexpected EPT violation. This erratum applies only if software enters 64-bit mode, loads CR3 with a 64-bit value, and then returns to 32-bit paging without changing CR3. Intel has not observed this erratum with any commercially available software.

Workaround: Software that has executed in 64-bit mode should reload CR3 with a 32-bit value before returning to 32-bit paging.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM66. Performance Monitor Events HLE_RETIREDA.BORTED_MISC4 And RTM_RETIREDA.BORTED_MISC4 May Over Count

Problem: The Performance Monitor Events HLE_RETIREDA.BORTED_MISC4 (Event C8H; Umask 40H) and RTM_RETIREDA.BORTED_MISC4 (Event C9H; Umask 40H) are defined to count the number of transactional aborts due to incompatible memory types. Due to this erratum, they may count additional unrelated transactional aborts.

Implication: The Performance Monitor Events HLE_RETIREDA.BORTED_MISC4 and RTM_RETIREDA.BORTED_MISC4 counts may be greater than the number of aborts due to incompatible memory types. This can result in nonzero counts when all memory types are compatible.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM67. A PCIe* LTR Update Message May Cause The Processor to Hang

Problem: If a PCIe device sends an LTR (Latency Tolerance Report) update message while the processor is in a package C6 or deeper, the processor may hang.

Implication: Due to this Erratum the processor may hang if a PCIe LTR update message is received while in a Package C6 or deeper.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

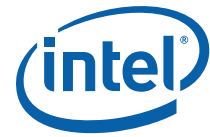
HSM68. GETSEC Does Not Report Support For S-CRTM

Problem: Processors with Intel® Boot Guard Technology that has GETSEC[PARAMETERS] leaf 5 EAX bit 5 set indicates support for processor rooted S-CRTM (Static Core Root of Trust for Measurement). Due to this erratum, that bit will not be set even though processor rooted S-CRTM is supported.

Implication: Software may be unaware of support for processor rooted S-CRTM.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.



HSM69. EPT Violations May Report Bits 11:0 of Guest Linear Address Incorrectly

Problem: If a memory access to a linear address requires the processor to update an accessed or dirty flag in a paging-structure entry and if that update causes an EPT violation, the processor should store the linear address into the "guest linear address" field in the VMCS. Due to this erratum, the processor may store an incorrect value into bits 11:0 of this field. (The processor correctly stores the guest-physical address of the paging-structure entry into the "guest-physical address" field in the VMCS.)

Implication: Software may not be easily able to determine the page offset of the original memory access that caused the EPT violation. Intel has not observed this erratum to impact the operation of any commercially available software.

Workaround: Software requiring the page offset of the original memory access address can derive it by simulating the effective address computation of the instruction that caused the EPT violation.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM70. APIC Timer Might Not Signal an Interrupt While in TSC-Deadline Mode

Problem: If the APIC timer is in TSC-deadline mode and is armed when a timed MWAIT instruction is executed, the timer expiration might not cause an interrupt.

Implication: Software depending on APIC timer TSC-deadline mode interrupts may not behave as expected.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM71. IA32_VMX_VMCS_ENUM MSR (48AH) Does Not Properly Report The Highest Index Value Used For VMCS Encoding

Problem: IA32_VMX_VMCS_ENUM MSR (48AH) bits 9:1 report the highest index value used for any VMCS encoding. Due to this erratum, the value 21 is returned in bits 9:1 although there is a VMCS field whose encoding uses the index value 23.

Implication: Software that uses the value reported in IA32_VMX_VMCS_ENUM[9:1] to read and write all VMCS fields may omit one field.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM72. Incorrect FROM_IP Value For an RTM Abort in BTM or BTS May be Observed

Problem: During RTM (Restricted Transactional Memory) operation when branch tracing is enabled using BTM (Branch Trace Message) or BTS (Branch Trace Store), 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, see the *Summary Table of Changes*.

**HSM73. VT-d Hardware May Perform STRP And SIRTTP Operations on a Package C7 Exit**

Problem: On a package C7 exit, VT-d hardware may spuriously perform SRTP (Set Root Table Pointer) and SIRTTP (Set Interrupt Remapping Table Pointer) operations. A package C7 exit can cause the value programmed by software in the RTA_REG (IRTA_REG) to be visible to hardware before software executes a GCMD.SRTP command. This will result in hardware using the new values for the DMA and interrupt translation page-walks, possibly before they are intended to be used by software.

Implication: If software has updated the root table pointer but has not executed the SRTP command then the root table pointer update will happen unexpectedly, causing the VMM to walk incorrect or non-existent tables. Intel has not observed this erratum with any commercially available software.

Workaround: Privileged software should not execute a MWAIT (because it can trigger a package C7 entry/exit) between writing to RTA_REG (IRTA_REG) and GCMD_REG.SRTP (GCMD_REG.SIRTTP) registers.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM74. General-Purpose Performance Counters Can Unexpectedly Increment

Problem: A performance monitor event programmed in a general-purpose performance counter should count the number of occurrences of the event selected in IA32_PERFVTSEL{0-7} MSR (186H-18DH). If INV (invert, bit 23) is set to 1 and a non-zero CMASK (Counter Mask) bits [31:24] value is used, due to this erratum, the event may over count in the case that either of OS (Operating System mode, bit 17) or USR (User mode, bit 16) is selected. Over counting will occur for the cycles spent in the non-matching CPL.

Implication: General-purpose performance counters may reflect counts higher than the actual number of events when the INV bit is set, CMASK is a non-zero value and either the OS or USR bit is set.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM75. Performance Monitoring Events May Report Incorrect Number of Load Hits or Misses to LLC

Problem: The following performance monitor events should count the numbers of loads hitting or missing LLC. However due to this erratum, The L3_hit related events may over count and the L3_miss related events may undercount.

MEM_LOAD_RETIRED.L3_HIT (Event D1H, Umask 40H)

MEM_LOAD_RETIRED.L3_MISS (Event D1H, Umask 20H)

MEM_LOAD_L3_HIT_RETIRED.XSNP_NONE (Event D2H, Umask 08H)

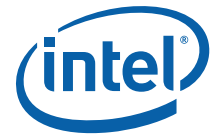
MEM_LOAD_LLC_MISS_RETIRED.LOCAL_DRAM (Event D3H, Umask 01H)

Implication: The listed performance monitoring events may be inaccurate.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM76. N/A. Erratum has been removed



HSM77. Locked Load Performance Monitoring Events May Under Count

Problem: The performance monitoring events MEM_TRANS_RETIRE.LOAD_LATENCY (Event CDH; Umask 01H), MEM_LOAD_RETIRE.L2_HIT (Event D1H; Umask 02H), and MEM_UOPS_RETIRE.LOCKED (Event DOH; Umask 20H) should count the number of locked loads. Due to this erratum, these events may under count for locked transactions that hit the L2 cache.

Implication: The above event count will under count on locked loads hitting the L2 cache.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM78. Processor May Hang Upon Entrance to Package C6 or C7

Problem: If the processor exits a Package C8 or deeper state without waking either the IA Cores or integrated graphics, a subsequent Package C6 or Package C7 entrance may hang.

Implication: Due to this erratum, when the processor attempts to enter Package C6 or Package C7 after exiting Package C8 or deeper states, it may hang.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM79. Graphics Processor Ratio And C-State Transitions May Cause a System Hang

Problem: If ratio or C-state changes involving the processor core and processor graphics occur at the same time or while processor graphics are active, under certain internal conditions the ratio change may not complete.

Implication: The system may hang during C-state or ratio changes.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM80. Certain Performance Monitoring Events May Over Count Software Demand Loads

Problem: The following performance monitor events should count the number of software demand loads. However due to this erratum, they may also include requests from the Next Page Prefetcher and over count.

OFFCORE_REQUESTS_OUTSTANDING.DEMAND_DATA (Event 60H; Umask 01H)

OFFCORE_REQUESTS.DEMAND_DATA (Event B0H; Umask 01H)

CYCLE_ACTIVITY.L2_Pending (Event A3H; Umask 01H)

L2_HIT_MISS.LOAD (Event 24H; Umask 01H)

Implication: The listed performance monitoring events may reflect a count higher than the actual number of events.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM81. Accessing Nonexistent Uncore Performance Monitoring MSRs May Not Signal a #GP**

Problem: An access to an uncore Performance Monitor MSR beyond the number reported in the MSR_UNC_CBO_CONFIG MSR (396H) bits[3:0] should signal a #GP (general-protection exception); due to this erratum, the processor may hang instead of signaling #GP.

Implication: When software accesses nonexistent uncore performance monitoring MSRs, the logical processor may hang instead of signaling a #GP.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM82. Power and Performance Regulation May Vary When Using RAPL

Problem: The processor power control algorithms using RAPL (Running Average Power Limits) may observe excessive power and performance ringing effects when a low power limit is used with time constant of greater than 6 seconds.

Implication: IA Core and integrated graphics frequencies and power consumption will have unexpected periodic fluctuations that do not settle.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM83. Call Stack Profiling May Produce Extra Call Records

Problem: The performance monitoring Call Stack Profiling function should not generate call records for “zero length calls” (call instructions targeting the location following the instruction). However, due to this erratum, the processor will produce call records for zero length calls.

Implication: The performance monitoring LBR call stack MSRs are incorrect in the presence of “zero length calls” because calls and returns do not match.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

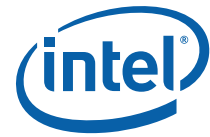
HSM84. Warm Reset May Fail or Lead to Incorrect Power Regulation

Problem: Due to this erratum, after a warm reset, the processor may fail to boot properly or may cause power to be regulated to an incorrect level.

Implication: The processor may not be able to control the VR (Voltage Regulator) to advertised specifications, leading to in a system hang, a machine check, or improper power regulation.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.



HSM85. PCIe* Host Bridge DID May Be Incorrect

Problem: The PCIe Host Bridge DID register (Bus 0; Device 0; Function 0; Offset 2H) contents may be incorrect.

Implication: Software that depends on the Host Bridge DID value may not behave as expected.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM86. Transactional Abort May Produce an Incorrect Branch Record

Problem: If an Intel® TSX transactional abort event occurs during a string instruction, the From-IP in the LBR (Last Branch Record) is not correctly reported.

Implication: Due to this erratum, an incorrect From-IP on the LBR stack may be observed.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM87. 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, see the *Summary Table of Changes*.

HSM88. TM1 Throttling Via IA32_CLOCK_MODULATION MSR May Hang

Problem: When TM1 throttling via the IA32_CLOCK_MODULATION MSR (19AH) with On-Demand Clock Modulation Enable bit 4 set and when Extended On-Demand Clock Modulation Duty Cycle bits [3:0] are programmed to a value of 1, a hang may occur.

Implication: Due to the erratum, a logical processor may hang.

Workaround: Extended On-Demand Clock Modulation Duty Cycle should be set to a value other than 1.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM89. DMA Remapping Faults for the Graphics VT-d Unit May Not Properly Report Type of Faulted Request

Problem: When a fault occurs during DMA remapping of Graphics accesses at the Graphics VT-d unit, the type of faulted request (read or write) should be reported in bit 126 of the FRCD_REG register in the remapping hardware memory map register set. Due to this erratum, the request type may not be reported correctly.

Implication: Software processing the DMA remapping faults may not be able to determine the type of faulting graphics device DMA request.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM90. Exiting Deep Package C-State May Result in a System Hang**

Problem: Due to this erratum, the processor may skip the dwell interval after ramping the external VR (Voltage Regulator) upon Package C8 or Package C9 exit.

Implication: VR behavior is undefined when the dwell interval is not met; issuing a VR ramp command during the dwell interval can result in unpredictable system behavior including a system hang.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM91. AVX Gather Instructions Page Faults May Report an Incorrect Faulting Address

Problem: If software modifies a paging-structure entry to relax the access rights for a linear address and does not perform a TLB invalidation, a subsequent execution of an AVX gather instruction that accesses that address may generate a page fault that loads CR2 (which should contain the faulting linear address) with an incorrect value.

Implication: Software handling an affected page fault may not operate correctly.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM92. N/A. Erratum has been removed**HSM93. Event Injection by VM Entry May Use an Incorrect B Flag for SS**

Problem: The stack accesses made by VM-entry event injection may use an incorrect value for the B flag (default stack-pointer size and upper bound) for the stack segment (SS).

Implication: An affected stack access may use an incorrect address or an incorrect segment upper bound. This may result in unpredictable system behavior.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

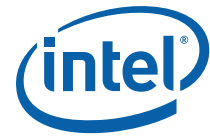
HSM94. LPDDR3 ZQ Calibration Following Deep Package C-state Exit May Lead to Unpredictable System Behavior

Problem: Due to this erratum, upon exit from Package C7 or deeper, the processor issues LPDDR3 ZQ calibration for dual die package or quad die package DRAMs in parallel instead of serially as required by the LPDDR3 spec for those devices.

Implication: A deep Package C-state exit on systems using LPDDR3 dual die package or quad die package DRAM may lead to unpredictable system behavior. Systems using LPDDR3 single die package DRAM or DDR3L memory are not affected.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM95. A Fault in SMM May Result in Unpredictable System Behavior**

Problem: The value of the SS register as well as the current privilege level (CPL) may be incorrect following a fault in SMM (system-management mode). The erratum can occur only if a fault occurs following an SMI (system-management interrupt) and before software has loaded the SS register (e.g., with the MOV SS instruction).

Implication: This erratum may cause unpredictable system behavior. Intel has not observed this erratum with any commercially available software.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM96. Processor Frequency is Unexpectedly Limited Below Nominal P1 When cTDP Down is Enabled

Problem: When cTDP (Configurable Thermal Design Power) Down is enabled on a processor branded as Core® i3 or Pentium®, the processor frequency will be limited to cTDP Down P1 frequency (Max Non-Turbo Frequency) when it should be able to operate between the cTDP Down frequency P1 and the nominal P1 frequency.

Implication: When cTDP is enabled, the processor cannot achieve expected frequencies.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM97. PMI May be Signaled More Than Once For Performance Monitor Counter Overflow

Problem: Due to this erratum, PMI (Performance Monitoring Interrupt) may be repeatedly issued until the counter overflow bit is cleared in the overflowing counter.

Implication: Multiple PMIs may be received when a performance monitor counter overflows.

Workaround: None identified. If the PMI is programmed to generate an NMI, software may delay the EOI (end-of- Interrupt) register write for the interrupt until after the overflow indications have been cleared.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM98. 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, see the *Summary Table of Changes*.

**HSM99. RDRAND Execution in a Transactional Region May Cause a System Hang**

Problem: Execution of the RDRAND (Random number generator) instruction inside an Intel® TSX transactional region may cause the logical processor to hang.

Implication: A system hang may occur as a result of this erratum.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM100. Intel® Turbo Boost Technology May be Incorrectly Reported as Supported on Intel® Core™ i3 U-series, Y-series and select Pentium® processors

Problem: The Intel Core™ i3 U-series, Y-series and select Pentium processors may incorrectly report support for Intel Turbo Boost Technology via CPUID.06H.EAX bit 1.

Implication: The CPUID instruction may report Turbo Boost Technology as supported even though the processor does not permit operation above the Maximum Non-Turbo Frequency.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM101. Uncore Clock Frequency Changes May Cause Audio/Video Glitches

Problem: On some processors, the time required to change the uncore clock frequency may be large enough to significantly lengthen the latency of I/O Requests to memory, possibly resulting in audio or video glitches.

Implication: Audio/Video glitches may occur during uncore ratio changes.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM102. Processor May Experience a Spurious LLC-Related Machine Check During Periods of High Activity

Problem: Due to certain internal conditions while running core and memory intensive operations, some processors may incorrectly report an LLC (last level cache) related machine check with a IA32_MCI_STATUS.MCACOD value of 110AH.

Implication: Due to this erratum, the processor may experience a machine check.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

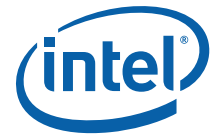
HSM103. The Processor May Not Enter Package C7 When Using a PSR Display

Problem: The processor datasheet specifies that entering package C7 requires enabling PSR (Panel Self Refresh) for certain display resolutions, along with other conditions. Due to this erratum, the processor may not enter package C7 when connected to a PSR-enabled display even if all of the required conditions are met.

Implication: Due to this erratum, the processor may not enter package C7.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM104. Video/Audio Distortion May Occur**

- Problem:** Due to this erratum, internal processor operations can occasionally delay the completion of memory read requests enough to cause video or audio streaming underrun.
- Implication:** Visible artifacts such as flickering on a video device or glitches on audio may occur.
- Workaround:** It is possible for the BIOS to contain a workaround for this erratum.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

HSM105. System May Hang When Audio is Enabled During Package C3

- Problem:** When audio is enabled while in package C3 state or deeper, audio memory traffic continues to be generated. Due to this erratum, the processor logic required for memory traffic may be powered down.
- Implication:** When this erratum occurs, the processor logic required for audio memory traffic may not be operational resulting in a system hang.
- Workaround:** It is possible for the BIOS to contain a workaround for this erratum.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

HSM106. INVPCID May Not Cause #UD in VMX Non-Root Operation

- Problem:** The INVPCID instruction should cause an invalid opcode exception (#UD) in VMX non-root operation if either bit 31 of the primary processor-based VM-execution controls (activate secondary controls) or bit 12 of the secondary processor-based VM-execution controls (enable INVPCID) is 0. Due to this erratum, the INVPCID instruction will not cause #UD if "activate secondary controls" is 0 and "enable INVPCID" is 1. Instead, the instruction will either execute normally or cause a VM exit if the "INVLPG exiting" VM-execution control is 1.
- Implication:** The processor may cause a VM exit that software does not expect. Intel has not observed this erratum with any commercially available software.
- Workaround:** None identified.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

HSM107. Non-Compliant PFAT Module Base Address May Cause Unpredictable System Behavior

- Problem:** PFAT (Platform Firmware Armoring Technology) requires the PFAT module base address be 256KB aligned and reside in the first 4GB of memory. If BIOS does not comply with these requirements when setting up the PFAT module, the processor should GP# at PFAT launch. Due to this erratum, a #GP fault may not be generated.
- Implication:** A PFAT module that does not follow the PFAT module base address requirements may result in unpredictable system behavior.
- Workaround:** It is possible for the BIOS to contain a workaround for this issue.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

**HSM108. Incorrect LBR Source Address May be Reported For a Transactional Abort**

Problem: If the fetch of an instruction in a transactional region causes a fault, a transactional abort occurs. If LBRs are enabled, the source address recorded for such a transactional abort is the address of the instruction being fetched. If that instruction was itself the target of an earlier branch instruction, this erratum may erroneously record the address of the branch instruction as the source address for the transactional abort.

Implication: Trace reconstruction software that uses LBR information may fail when this erratum occurs.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM109. Address Translation Faults for Intel® VT-d May Not be Reported for Display Engine Memory Accesses

Problem: The Intel® VT-d (Intel® Virtualization Technology for Directed I/O) hardware unit supporting the Processor Graphics device (Bus 0; Device 2; Function 0) may not report address translation faults detected on Display Engine memory accesses when the Context Cache is disabled or during time periods when Context Cache is being invalidated.

Implication: Due to this erratum, Display Engine accesses that fault are correctly aborted but may not be reported in the FSTS_REG fault reporting register (GFXVTDBAR offset 034H).

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM110. L3 Cache Corrected Error Count May be Inaccurate After Package C7 Exit

Problem: The corrected error count for L3 cache errors reported in IA32_MCI_STATUS.Corrected Error Count (bits [52:38]) with an MCACOD of 0001 0001 xxxx xxxx (x can be 0 or 1) may be incorrectly restored to a smaller value during exit from Package C7.

Implication: The corrected error count for L3 cache errors in IA32_MCI_STATUS may be inaccurate after Package C7 exit.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

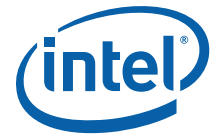
HSM111. PCIe* Device's SVID is Not Preserved Across The Package C7 C-State

Problem: Bus 0, Device 7, Function 0's SVID register (Subsystem Vendor Identification, Offset 2CH) is not preserved across package C7 C-State transitions.

Implication: This may cause the operating system to think the device has been replaced with a different device.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM112. Warm Reset Does Not Stop GT Power Draw**

Problem: Due to this erratum, if GT is enabled prior to a warm reset, it will remain powered after the warm reset. The processor will make incorrect power management decisions because it assumes the GT is not drawing power after a warm reset.

Implication: The processor may draw more current than expected from an external VR (Voltage Regulator). The processor may also put the external VR into a low power state where it will be unable to supply the sufficient power resulting in unpredictable system behavior.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM113. Unused PCIe* Lanes May Remain Powered After Package C7

Problem: If a PCIe controller is enabled and either has unused lanes or no PCIe device is present, the link and/or unused lanes should enter a low power state. Due to this erratum, after exiting Package C7, the unused link and/or unused lanes may remain powered.

Implication: Power consumption may be greater than expected.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM114. BMI1 And BMI2 Instruction Groups Are Not Available

Problem: Feature flags BMI1 and BMI2 (CPLD leaf 7, sub-leaf 0, EBX bits 3 and 8) report these two groups of bit manipulation instructions are not present for Intel® Core™ i3-4100M these instruction groups should be available. An attempt to execute any of these instructions will generate a #UD fault.

Implication: Software attempting to use any of instructions in the BMI1 and BMI2 groups will result in a #UD fault

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM115. HD Audio Device Playback May Be Interrupted if The Processor Enters a Deep Package C-State

Problem: When the Integrated Graphics Device (Bus 0; Device 2; Function 0) is in the D3 state, the processor may enter package C8 or deeper C-state, shutting down the Display Engine in the process. However, Display Engine operation may be required by the HD Audio device (Bus 0; Device 3; Function 0).

Implication: When this erratum occurs the audio controller may reset causing audio playback to stop and be unable to resume.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM116. Virtual-APIC Page Accesses With 32-Bit PAE Paging May Cause a System Crash**

Problem: If a logical processor has EPT (Extended Page Tables) enabled, is using 32-bit PAE paging, and accesses the virtual-APIC page then a complex sequence of internal processor micro-architectural events may cause an incorrect address translation or machine check on either logical processor.

Implication: This erratum may result in unexpected faults, an uncorrectable TLB error logged in IA32_MCI_STATUS.MCACOD (bits [15:0]) with a value of 0000_0000_0001_xxxx**b** (where x stands for 0 or 1), a guest or hypervisor crash, or other unpredictable system behavior.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM117. Processor Energy Policy Selection May Not Work as Expected

Problem: When the IA32_ENERGY_PERF_BIAS MSR (1B0H) is set to a value of 4 or more, the processor will try to increase the energy efficiency of Turbo mode. However, this functionality is effectively disabled if the software requested P-state exceeds the maximum P-state supported by the processor. This has the effect of decreasing the energy efficiency of the processor while in Turbo mode.

Implication: When this erratum occurs, reduced battery life and reduced energy efficiency may occur.

Workaround: BIOS should set the max ACPI _PST object to the max supported turbo ratio, ensuring that the software P-state request does not exceed the maximum ratio supported by the processor. Note that this workaround will disable Core Ratio Overclocking.

Status: For the steppings affected, see the *Summary Table of Changes*.

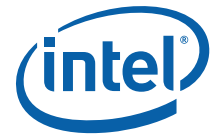
HSM118. Processor May Not be Able to Reduce The Graphics Engine's Effective Frequency

Problem: The processor may be unable to reduce the effective frequency of the graphics engine in response to a power or thermal event.

Implication: Due to this erratum, the processor may be unable to reduce power consumption to the power target specified by the platform embedded controller or software. This may result in reduced battery life and/or a platform temperature excursion.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.



HSM119. A PEBS Record May Contain Processor State for an Unexpected Instruction

Problem: If a performance counter has overflowed and is configured for PEBS (precise event-based sampling), the processor will arm the PEBS hardware within a bounded number of cycles called the skid (see the discussion of skid and related topics in the Precise Distribution of Instructions Retired section of the Intel® 64 and IA-32 Architectures Software Developer Manual). Once the PEBS hardware is armed, the processor should capture processor state in a PEBS record following the execution of the next instruction that causes the counter to increment (a “triggering” instruction). Due to this erratum, the capture of processor state may occur at an instruction after the first triggering instruction following the skid but not beyond the second triggering instruction after the skid.

Implication: A PEBS record may contain processor state (including instruction pointer) not associated with the triggering instruction.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM120. MSR_PP1_ENERGY_STATUS Reports Incorrect Energy Data

Problem: The MSR_PP1_ENERGY_STATUS MSR (641H) bits [31:0] reports incorrect energy data.

Implication: Due to this erratum, reported Intel Integrated Graphics domain energy consumption may not be accurate.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM121. x87 FPU DP May be Incorrect After Instructions That Save FP State to Memory

Problem: Under certain conditions, the value of the x87 FPU DP (Floating Point Unit Data Pointer) saved by the FSAVE/FNSAVE, FSTENV/FNSTENV, FXSAVE, XSAVE, or XSAVEOPT instructions may be incorrect.

Implication: Due to this erratum, the x87 FPU DP may be incorrect.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM122. Processor May Hang During Package C7 Exit

Problem: Under certain internal timing conditions, the processor might not properly exit package C7 leading to a hang.

Implication: Due to this erratum, the package C7 state may not be reliable. Intel has not observed this erratum with any commercially available system.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.



HSM123. Certain Processors May Experience Transient LLC ECC Errors

Problem: Due to certain internal conditions while running core, graphics and memory intensive operations, some processors may report LLC (last level cache) ECC errors, with IA32_MCI_STATUS[15:0] MCACOD reporting a Cache Hierarchy Error (000F 0001 RRRR TT10) and IA32_MCI_STATUS[31:16] MSCOD with value 0000 0000 0000 1000.

Implication: When this erratum occurs, an uncorrectable LLC error will be logged and the system may hang or restart.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM124. N/A. Erratum has been removed

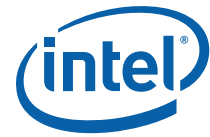
HSM125. Spurious LLC Machine Check May Occur

Problem: Under certain stressful conditions while running at ring ratios higher than 30, the processor may experience a spurious LLC machine check as indicated by IA32_MCI_STATUS.MCACOD (bits [15:0]) with value 000x 0001 0000 1010 (where x is 0 or 1).

Implication: When this erratum occurs, an uncorrectable LLC error will be logged and the system may hang or restart.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.



HSM126. Page Fault May Report Incorrect Fault Information

Problem: Under the following conditions:

1. A read-modify-write instruction's memory source/destination (e.g., ADD memory, reg) crossing a cache line boundary.
2. That instruction executing without fault.
3. While the read-modify-write instruction is executing, one or more of the following page table attributes associated with its memory operand are modified:
 - a. The D (dirty) flag was 0 when the instruction was initiated but was concurrently set to 1, and/or
 - b. One of the relevant R/W flags was 0 when the instruction was initiated but was concurrently set to 1, and/or
 - c. If the read-modify-write instruction executes at CPL = 3 and one of the relevant U/S flags was 0 when the instruction was initiated but was concurrently set to 1.
4. A subsequent instruction executing within a narrow timing window that experiences a page fault.
5. There is no serializing instruction between the read-modify-write instruction and the faulting instruction.

The page fault (in #4) may report an incorrect error code and faulting linear address; these would describe the read-modify-write instruction's memory access instead of that of the faulting instruction. (The address of the faulting instruction is reported correctly.)

Implication: The erratum makes it appear that the page fault resulted from an access that occurred prior to the faulting instruction. Because the earlier access completed without faulting, a page-fault handler may identify the page fault as transient (or spurious) and re-execute the faulting instruction (e.g., by executing IRET). In such cases, the erratum will not recur; the page fault on the later access will recur and will be reported correctly. If the page-fault handler does not re-execute the faulting instruction, this erratum may result in unpredictable system behavior. Intel has not observed this erratum with any commercially available software.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM127. CATERR# Pin Assertion is Not Cleared on a Warm Reset

Problem: If the CATERR# pin is held asserted to indicate a fatal error, a subsequent warm reset event will not cause the CATERR# pin to de-assert.

Implication: When this erratum occurs, platforms that monitor the CATERR# pin may be unable to detect a fatal error after a warm reset or may incorrectly respond to a CATERR# pin assertion although an error may not have occurred subsequent to the warm reset event.

Workaround: The CATERR# pin can be de-asserted by a cold reset event.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM128. Uncorrectable Machine Check Error During Core C6 Entry May Not be Signaled**

Problem: Machine Check exceptions occurring during core C6 entry may be ignored.

Implication: When this erratum occurs, incorrect state may be saved during core C6 entry and subsequently restored during core C6 exit resulting in unpredictable system behavior.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM129. The SAMPLE/PRELOAD JTAG Command Does Not Sample The Display Transmit Signals

Problem: The Display Transmit signals are not correctly sampled by the SAMPLE/PRELOAD JTAG Command, violating the Boundary Scan specification (IEEE 1149.1).

Implication: The SAMPLE/PRELOAD command cannot be used to sample Display Transmit signals.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM130. Performance Monitor Event For Outstanding Offcore Requests And Snoop Requests May be Incorrect

Problem: The performance monitor event OFFCORE_REQUESTS_OUTSTANDING (Event 60H, any Umask Value) should count the number of offcore outstanding transactions each cycle. Due to this erratum, the counts may be higher or lower than expected.

Implication: The performance monitor event OFFCORE_REQUESTS_OUTSTANDING may reflect an incorrect count.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM131. Processor Energy Policy Selection May Not Work as Expected

Problem: When the IA32_ENERGY_PERF_BIAS MSR (1B0H) is set to a value of 4 or more, the processor will try to increase the energy efficiency of Turbo mode. However, this functionality is effectively disabled if the software requested P-state exceeds the maximum P-state supported by the processor.

Implication: When this erratum occurs, the energy efficiency control may not behave as expected.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

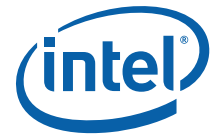
HSM132. PCIe Link May Incorrectly Train to 8.0 GT/s

Problem: During PCIe* 8.0 GT/s Phase 2 Equalization training, the received per-lane transmitter coefficients for physical lanes 8-15 may be incorrectly applied to the PCIe transmitters.

Implication: Due to this erratum, a PCIe link may either fail to train to the 8.0 GT/s transfer speed, experience link errors, or periodically retrain (possibly dropping to a lower link speed).

Workaround: A BIOS code change has been identified and may be implemented as a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.



HSM133. PCIe Tx Voltage Reference Cannot be Changed

Problem: PCIe* Tx Voltage Reference Select is available via the PCIE_CR_AFEBCND[0:7]CFG1 (Device 1; Function 0) registers in field TxVrefSel bits [9:5]. Due to this erratum, changes to these values will have no effect.

Implication: For PCIe, setting the Tx Voltage Reference Select to non-default values will not produce the reference levels documented in the register description. Tx swing control utilizes Tx Voltage Reference; Tx swing cannot be adjusted from default.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM134. VM Exit May Set IA32_EFER.NXE When IA32_MISC_ENABLE Bit 34 is Set to 1

Problem: When "XD Bit Disable" in the IA32_MISC_ENABLE MSR (1A0H) bit 34 is set to 1, it should not be possible to enable the "execute disable" feature by setting IA32_EFER.NXE. Due to this erratum, a VM exit that occurs with the 1-setting of the "load IA32_EFER" VM-exit control may set IA32_EFER.NXE even if IA32_MISC_ENABLE bit 34 is set to 1. This erratum can occur only if IA32_MISC_ENABLE bit 34 was set by guest software in VMX non-root operation.

Implication: Software in VMX root operation may execute with the "execute disable" feature enabled despite the fact that the feature should be disabled by the IA32_MISC_ENABLE MSR. Intel has not observed this erratum with any commercially available software.

Workaround: A virtual-machine monitor should not allow guest software to write to the IA32_MISC_ENABLE MSR.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM135. Re-enabling eDRAM May Log a Machine Check and Hang

Problem: If the eDRAM was disabled as a result of a package C-State entry of C2 or higher or a software request, the subsequent package C-state exit or software request to re-enable eDRAM may result in a machine check logged in IA32_MCI_STATUS.MCACOD [15:0] with of value 402H and subsequent system hang.

Implication: Due to this erratum, the system may log a machine check and hang.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM136. Warm Reset Does Not Stop EDRAM Power Draw

Problem: Due to this erratum, if EDRAM is enabled prior to a warm reset, it will remain powered after the warm reset. The processor will make incorrect power management decisions because it assumes the EDRAM is not drawing power after a warm reset.

Implication: The processor may draw more current than expected from an external VR (Voltage Regulator). The processor may also put the external VR into a low power state where it will be unable to supply the sufficient power resulting in unpredictable system behavior.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM137. CHAP Counter Values May be Cleared After Package C7 or Deeper C-State**

Problem: The CHAP (Chipset Hardware Architecture Performance) counters which do not have a "Start" OpCode present in the CMD register will not be preserved across a Package C7 or deeper C-State.

Implication: CHAP Counter data is not saved/restored after Package C7 or deeper C-state causing counts to be lost; actions based on those counts may not occur as expected.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM138. Opcode Bytes F3 0F BC May Execute As TZCNT Even When TZCNT Not Enumerated by CPUID

Problem: If CPUID.(EAX=07H, ECX=0):EBX.BMI1 (bit 3) is 1 then opcode bytes F3 0F BC should be interpreted as TZCNT otherwise they will be interpreted as REP BSF. Due to this erratum, opcode bytes F3 0F BC may execute as TZCNT even if CPUID.(EAX=07H, ECX=0):EBX.BMI1 (bit 3) is 0.

Implication: Software that expects REP prefix before a BSF instruction to be ignored may not operate correctly since there are cases in which BSF and TZCNT differ with regard to the flags that are set and how the destination operand is established.

Workaround: Software should use the opcode bytes F3 0F BC only if CPUID.(EAX=07H, ECX=0):EBX.BMI1 (bit 3) is 1 and only if the functionality of TZCNT (and not BSF) is desired.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM139. Intel® S2DDT May Not Function Correctly with Certain High Resolution Displays

Problem: A limitation in Intel S2DDT (Intel® Smart 2D Display Technology), commonly known as frame buffer compression, may result in pixel data being supplied too slowly to the display.

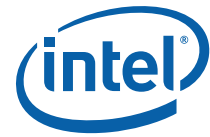
Implication: Screen flickering or blank screen may be observed on certain high resolution displays.

Workaround: The latest version of the Intel graphics driver disables Intel S2DDT for resolutions with a pixel clock listed below:

Affected Intel® Processor	Affected Pixel Clock Rate
4 th Generation Intel® Core™ H-Processor Line and 4 th Generation Intel® Core™ M-Processor Line	Between 513 and 540 MHz
4 th Generation Intel® Core™ U-Processor Line	Between 427.5 and 450 MHz
4 th Generation Intel® Core™ Y-Processor Line	Between 320.625 and 337.5 MHz

Status: For the steppings affected, see the *Summary Table of Changes*

HSM140. N/A. Errata has been Removed

**HSM141. VM Exit May Set IA32_EFER.NXE When IA32_MISC_ENABLE Bit 34 is Set to 1**

Problem: When “XD Bit Disable” in the IA32_MISC_ENABLE MSR (1A0H) bit 34 is set to 1, it should not be possible to enable the “execute disable” feature by setting IA32_EFER.NXE. Due to this erratum, a VM exit that occurs with the 1-setting of the “load IA32_EFER” VM-exit control may set IA32_EFER.NXE even if IA32_MISC_ENABLE bit 34 is set to 1. This erratum can occur only if IA32_MISC_ENABLE bit 34 was set by guest software in VMX non-root operation.

Implication: Software in VMX root operation may execute with the “execute disable” feature enabled despite the fact that the feature should be disabled by the IA32_MISC_ENABLE MSR. Intel has not observed this erratum with any commercially available software.

Workaround: A virtual-machine monitor should not allow guest software to write to the IA32_MISC_ENABLE MSR.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM142. Spurious Corrected Errors May be Reported

Problem: Due this erratum, spurious corrected errors may be logged in the IA32_MC0_STATUS register with the valid field (bit 63) set, the uncorrected error field (bit 61) not set, a Model Specific Error Code (bits [31:16]) of 0x000F, and an MCA Error Code (bits [15:0]) of 0x0005. If CMCI is enabled, these spurious corrected errors also signal interrupts.

Implication: When this erratum occurs, software may see corrected errors that are benign. These corrected errors may be safely ignored.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM143. A MOV to CR3 When EPT is Enabled May Lead to an Unexpected Page Fault or an Incorrect Page Translation

Problem: If EPT (extended page tables) is enabled, a MOV to CR3 or VMFUNC may be followed by an unexpected page fault or the use of an incorrect page translation.

Implication: Guest software may crash or experience unpredictable behavior as a result of this erratum.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM144. Package C7 Power Consumption Has Been Observed to be Higher Than Package C6

Problem: Package C7 power consumption may be higher than package C6 power consumption.

Implication: When this erratum occurs, power consumption will be higher than expected.

Workaround: It is possible for the BIOS to contain a workaround for this erratum which demotes package C7 to package C6 when power consumption in package C7 is likely to be higher than in package C6.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM145. A HyperThreading Enabled Processor May Exhibit Unpredictable Behavior During Power or Thermal Management Operations**

Problem: When both logical processors in a core are idled due to power or thermal management operations such as thermal events or C-state entry, under certain circumstances, instruction fetches initiated before entering the idle state may not complete correctly, resulting in unpredictable system behavior.

Implication: Due to this erratum, the processor may exhibit 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, see the *Summary Table of Changes*.

HSM146. Certain Perfmon Events May be Counted Incorrectly When The Processor is Not in C0 State

Problem: Due to this erratum, the perfmon events listed below may be counted when the logical processor is not in C0 State.

IDQ.EMPTY (event code 0x79 and umask 0x02)

IDQ_UOPS_NOT_DELIVERED.CORE (event code 0x9c and umask 0x01)

RESOURCE_STALLS.ANY (event code 0xa2 umask 0x01)

CYCLE_ACTIVITY.CYCLES_LDM_PENDING (Event A3H, Umask 02H, Cmask 02H)

CYCLE_ACTIVITY.CYCLES_NO_EXECUTE (Event A3H, Umask 04H, Cmask 04H)

CYCLE_ACTIVITY.STALLS_LDM_PENDING (Event A3H, Umask 06H, Cmask 06H)

Implication: The count will be higher than expected.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM147. System Hang May Occur During Exit From Package C7 Due to VccST sensitivity

Problem: Due to this erratum, a VccST sensitivity may cause the processor to hang while exiting from package C7 state.

Implication: Due to this erratum, a system hang may occur.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

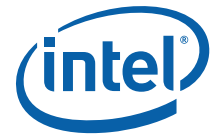
HSM148. Software Using Intel® TSX May Result in Unpredictable System Behavior

Problem: Under a complex set of internal timing conditions and system events, software using the Intel TSX (Transactional Synchronization Extensions) instructions may result in unpredictable system behavior.

Implication: This erratum may result in unpredictable system behavior.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM149. Running All Cores May Incorrectly Limit the Processor Frequency**

Problem: When all IA cores in the processor are running but not executing AVX instructions and the processor is not constrained by PL1/PL2 power limits or thermal limits, the cores should be able to operate at the 4C turbo frequency. Due to this erratum, the processor may limit core frequency under these conditions as much as several bins below the 4C turbo frequency.

Implication: When this erratum occurs, the processor will not meet specified performance levels.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM150. Concurrent Core And Graphics Operation at Turbo Ratios May Lead to System Hang

Problem: Workloads that attempt concurrent operation of cores and graphics in their respective turbo ranges, under certain conditions may result in a system hang.

Implication: Concurrent core and graphics operation may hang the system

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM151. Performance Monitor Instructions Retired Event May Not Count Consistently

Problem: Performance Monitor Instructions Retired (Event C0H; Umask 00H) and the instruction retired fixed counter (IA32_FIXED_CTR0 MSR (309H)) are used to track the number of instructions retired. Due to this erratum, certain situations may cause the counter(s) to increment when no instruction has retired or to not increment when specific instructions have retired.

Implication: A performance counter counting instructions retired may over or under count. The count may not be consistent between multiple executions of the same code.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM152. Some Configurations May Violate Embedded DRAM Refresh Requirements Leading to a System Hang

Problem: Due to this erratum, embedded DRAM refresh requirements may be violated for some configurations leading to memory errors.

Implication: When this erratum occurs, the resulting memory errors may cause a system shutdown or hang.

Workaround: It is possible for BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM153. Interactions Between Multiple Unaligned Memory Accesses And Locked Instructions May Lead to a Machine Check**

Problem: Under a complex set of conditions, interactions between multiple locked operations sharing certain low order address bits and data accesses that span a 4-KByte boundary may result in a processor internal timeout machine check (IA32_MCI_STATUS.MCACOD = 0x0400).

Implication: Due to this erratum, the processor may signal a machine check exception. Intel has not observed this erratum with any commercially available system.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM154. Fixed-Function Performance Counter May Over Count Instructions Retired by 32 When Intel® Hyper-Threading Technology is Enabled

Problem: If, while Intel Hyper-Threading Technology is enabled, the IA32_FIXED_CTR0 MSR (309H) is enabled by setting bits 0 and/or 1 in the IA32_PERF_FIXED_CTR_CTRL MSR (38DH) before setting bit 32 in the IA32_PERF_GLOBAL_CTRL MSR (38FH) then IA32_FIXED_CTR0 may over count by up to 32.

Implication: When this erratum occurs, the fixed-function performance counter IA32_FIXED_CTR0 may over count by up to 32.

Workaround: The following sequence avoids this erratum (steps 1 and 2 are needed if the counter was previously enabled):

1. Clear bit 32 in the IA32_PERF_GLOBAL_CTRL MSR (38FH) and clear bits 1 and 0 in the IA32_PERF_FIXED_CTR_CTRL MSR (38DH).
2. Zero the IA32_FIXED_CTR0 MSR.
3. Set bit 32 in the IA32_PERF_GLOBAL_CTRL MSR.
4. Set bits 0 and/or 1 in the IA32_PERF_FIXED_CTR_CTRL MSR as desired.

Status: For the steppings affected, see the *Summary Table of Changes*.

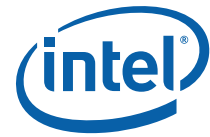
HSM155. Performance Monitor UOPS_EXECUTED Event May Be Inaccurate When Using Intel® Hyper-Threading Technology

Problem: The performance monitor event UOPS_EXECUTED (Event B1H, Umask 01H) counts the number of uops executed each cycle. However, due to this erratum, when using Intel Hyper-Threading Technology, the uops may not be assigned to the correct logical processor.

Implication: The total number of uops executed by a core will be counted correctly but the division of uops between its logical processors may be incorrect.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.



HSM156. Operand-Size Override Prefix Causes 64-bit Operand Form of MOVBE Instruction to Cause a #UD

Problem: Execution of a 64 bit operand MOVBE instruction with an operand-size override instruction prefix (66H) may incorrectly cause an invalid-opcode exception (#UD).

Implication: A MOVBE instruction with both REX.W=1 and a 66H prefix will unexpectedly cause an invalid-opcode exception (#UD). Intel has not observed this erratum with any commercially available software

Workaround: Do not use a 66H instruction prefix with a 64-bit operand MOVBE instruction.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM157. POPCNT Instruction May Take Longer to Execute Than Expected

Problem: POPCNT instruction execution with a 32 or 64 bit operand may be delayed until previous non-dependent instructions have executed.

Implication: Software using the POPCNT instruction may experience lower performance than expected.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM158. System May Hang or Video May be Distorted After Graphics RC6 Exit

Problem: In a specific scenario, when the processor graphics exits RC6 and a processor core exits C6 at the same time, the system may become unresponsive or the video may become distorted.

Implication: The system may hang or video may be distorted.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM159. Certain eDP* Displays May Not Function as Expected

Problem: When the processor attempts to receive data on the eDP AUX bus, the impedance seen by the display's AUX bus drivers will be significantly below the VESA* eDP (Embedded DisplayPort*) specification's requirement for the Vaux(Rx) (eDP Auxiliary Channel) input impedance.

Implication: Certain eDP displays may not operate as expected.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM160. Some OFFCORE_RESPONSE Performance Monitoring Events May Undercount

Problem: The performance monitoring events OFFCORE_RESPONSE (Events B7H and BBH) should count uncore responses matching the request-response configuration specified in MSR_OFFCORE_RSPs (1A6H and 1A7H, respectively) for core-originated requests. However due to this erratum, COREWB (bit 3), PF_L3_DATA_RD (bit 7), PF_L3_RFO (bit 8), PR_L3_CODE_RD (bit 9), SPLIT_LOCK_UC_LOCK (bit 10), and STREAMING_STORES (bit 11) request types may undercount.

Implication: These performance monitoring events may not produce reliable results for the listed request types.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM161. Certain Settings of VM-Execution Controls May Result in Incorrect Linear-Address Translations**

- Problem:** If VM exit occurs from a guest with primary processor-based VM-execution control “activate secondary controls” set to 0 and the secondary processor-based VM-execution control “enable VPID” set to 1, then after a later VM entry with VPID fully enabled (“activate secondary controls” and “enable VPID” set to 1), the processor may use stale linear address translations.
- Implication:** The processor may incorrectly translate linear addresses. Intel has not observed this erratum with any commercially available software.
- Workaround:** Software should not enter a guest with “enable VPID” set to 1 when “activate secondary controls” is set to 0.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

HSM162. An IRET Instruction That Results in a Task Switch Does Not Serialize The Processor

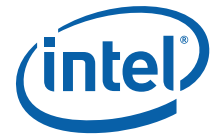
- Problem:** An IRET instruction that results in a task switch by returning from a nested task does not serialize the processor (contrary to the Software Developer’s Manual Vol. 3 section titled “Serializing Instructions”).
- Implication:** Software which depends on the serialization property of IRET during task switching may not behave as expected. Intel has not observed this erratum to impact the operation of any commercially available software.
- Workaround:** None identified. Software can execute an MFENCE instruction immediately prior to the IRET instruction if serialization is needed.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

HSM163. Attempting to Disable Turbo Mode May Cause a #GP

- Problem:** Bit 38 of IA32_MISC_ENABLE MSR (1A0H) is Turbo Mode Disable on processors that support Intel® Dynamic Acceleration. Due to this erratum, that bit may be incorrectly treated as reserved; attempting to set Turbo Mode Disable results in a #GP (General Protection exception) even when it reads as 1.
- Implication:** When this erratum occurs, a WRMSR to IA32_MISC_ENABLE unexpectedly causes a #GP.
- Workaround:** It is possible for BIOS to contain a workaround for this erratum.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

HSM164. Machine Check Threshold Based Error Status May be Set Incorrectly

- Problem:** A corrected error may be logged in IA32_MCI_STATUS with the Threshold Based Error field (bits[54:53]) indicating yellow status (10b) although the part is not above the threshold.
- Implication:** This erratum may be associated with a Cache Hierarchy Error reported in the Compound Error Code (bits[15:0]) of IA32_MCI_STATUS in the form 000F 0001 RRRR TTLL where LL is 11 and there are valid values for the other sub-fields (F, RRRR, and TT).
- Workaround:** None identified. A power-on reset of the processor will clear the yellow bit indication. If, during system operation after that reset, yellow status is signaled again then it should be treated as a valid yellow status condition.
- Status:** For the steppings affected, see the *Summary Table of Changes*.



HSM165. PECI Frequency Limited to 1 MHz

Problem: The Peci (Platform Environmental Control Interface) 3.1 specification's operating frequency range is 0.2 MHz to 2 MHz. Due to this erratum, Peci may be unreliable when operated above 1 MHz.

Implication: Platforms attempting to run Peci above 1 MHz may not behave as expected.

Workaround: None identified. Platforms should limit Peci operating frequency to 1 MHz.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM166. VGATHERQPS That Loads an Element From The APIC-Access Page May Load Other Elements From Incorrect Addresses

Problem: If the "virtualize APIC accesses" VM-execution control is 1, a 256-bit VGATHERQPS with an element that maps to the APIC-access page may use incorrect addresses to load other elements.

Implication: Loading from an incorrect address can result in unexpected behavior with respect to data, faults or VM exits. This erratum will occur only if a guest operating system attempts to access the APIC using the VGATHERQPS instruction. Intel has not observed this erratum with any commercially available software.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM167. MTF VM Exit on XBEGIN Instruction May Save State Incorrectly

Problem: Execution of an XBEGIN instruction while the "monitor trap flag" VM-execution control is 1 will be immediately followed by an MTF VM exit. If advanced debugging of RTM transactional regions has been enabled, the VM exit will erroneously save the address of the XBEGIN instruction as the instruction pointer (instead of the fallback instruction address specified by the XBEGIN instruction). In addition, it will erroneously set bit 16 of the pending-debug-exceptions field in the VMCS indicating that a debug exception or a breakpoint exception occurred.

Implication: Software using the monitor trap flag to debug or trace transactional regions may not operate properly. Intel has not observed this erratum with any commercially available software.

Workaround: None identified

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM168. Uncore Performance Monitoring Counters May be Disabled or Cleared After Package C7

Problem: Upon exiting Package C7, the following Uncore performance monitoring MSRs may be cleared to zero:

- MSR_UNC_PERF_GLOBAL_CTRL (391H)
- MSR_UNC_PERF_GLOBAL_STATUS (392H)
- MSR_UNC_PERF_FIXED_CTRL (394H)
- MSR_UNC_PERF_FIXED_CTR (395H)

Implication: Uncore performance monitoring counters may be disabled and some counter state may be cleared after Package C7.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM169. PEBS Record May Be Generated After Being Disabled**

- Problem:** A performance monitoring counter may generate a PEBS (Precise Event Based Sampling) record after disabling PEBS or the performance monitoring counter by clearing the corresponding enable bit in IA32_PEBS_ENABLE MSR (3F1H) or IA32_PERF_GLOBAL_CTRL MSR (38FH).
- Implication:** A PEBS record generated after a VMX transition will store into memory according to the post-transition DS (Debug Store) configuration. These stores may be unexpected if PEBS is not enabled following the transition.
- Workaround:** It is possible for the BIOS to contain a workaround for this erratum. A software workaround is possible through disallowing PEBS during VMX non-root operation and disabling PEBS prior to VM entry.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

HSM170. PCIe* Ports Do Not Support DLL Link Active Reporting

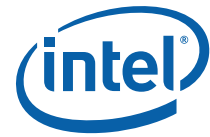
- Problem:** The PCIe Base Specification requires every "Downstream Port that supports Link speeds greater than 5.0 GT/s" to support DLL (Data Link Layer) Link Active Reporting. However, the PCIe ports do not support DLL Link Active Reporting.
- Implication:** Due to this erratum, the PCIe ports do not support DLL Link Active Reporting. This may be reported by a PCIe compliance test.
- Workaround:** None identified.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

HSM171. PCIe* Link Speed Negotiation May Fail After Link is Re-enabled

- Problem:** If a PCIe link is established then disabled and the link partner's advertised speeds are changed while the link is disabled, the link may fail to correctly negotiate link speed when it is re-enabled.
- Implication:** Due to this erratum, the PCIe link speed negotiation may fail after re-enabling a disabled port.
- Workaround:** None identified.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

HSM172. MOVNTDQA From WC Memory May Pass Earlier Locked Instructions

- Problem:** An execution of (V)MOVNTDQA (streaming load instruction) that loads from WC (write combining) memory may appear to pass an earlier locked instruction that accesses a different cache line.
- Implication:** Software that expects a lock to fence subsequent (V)MOVNTDQA instructions may not operate properly.
- Workaround:** None identified. Software that relies on a locked instruction to fence subsequent executions of (V)MOVNTDQA should insert an MFENCE instruction between the locked instruction and subsequent (V)MOVNTDQA instruction.
- Status:** For the steppings affected, see the *Summary Table of Changes*.

**HSM173. Data Breakpoint Coincident With a Machine Check Exception May be Lost**

Problem: If a data breakpoint occurs coincident with a machine check exception, then the data breakpoint may be lost.

Implication: Due to this erratum, a valid data breakpoint may be lost.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM174. A Corrected Internal Parity Error May Result in a System Hang

Problem: A corrected Internal Parity Error (IA32_MC0_STATUS.MCACOD=0005H and IA32_MC0_STATUS.MSCOD=000FH, MSR 401H bits [15:0] and bits [31:16] respectively) may cause a system hang.

Implication: Due to this erratum, a corrected internal parity error may cause a system hang. Reset, SMI, or INIT will end the system hang.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM175. An APIC Timer Interrupt During Core C6 Entry May Be Lost

Problem: Due to this erratum, an APIC timer interrupt coincident with the core entering C6 state may be lost rather than held for servicing later.

Implication: A lost APIC timer interrupt may lead to missed deadlines or a system hang.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM176. Internal Power State Transitions May Cause the Graphics Device to Hang

Problem: On certain processors, when the graphics device transitions among active power states in response to dynamic power demand, the graphics device may become unresponsive.

Implication: When this erratum occurs, the graphics device may hang, resulting in a frozen or blank display. The graphics driver may be able to restart the graphics device.

Workaround: It is possible for BIOS to contain processor configuration data and code changes as a workaround for this erratum.

Status: For the steppings affected, see the *Summary Table of Changes*.



HSM177. PEBS EventingIP Field May Be Incorrect Under Certain Conditions

Problem: The EventingIP field in the PEBS (Processor Event-Based Sampling) record reports the address of the instruction that triggered the PEBS event. Under certain complex microarchitectural conditions, the EventingIP field may be incorrect.

Implication: When this erratum occurs, performance monitoring software may not attribute the PEBS events to the correct instruction.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

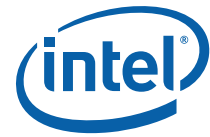
HSM178. RF May be Incorrectly Set in The EFLAGS That is Saved on a Fault in PEBS or BTS

Problem: After a fault due to a failed PEBS (Processor Event Based Sampling) or BTS (Branch Trace Store) address translation, the RF (resume flag) may be incorrectly set in the EFLAGS image that is saved.

Implication: When this erratum occurs, a code breakpoint on the instruction following the return from handling the fault will not be detected. This erratum only happens when the user does not prevent faults on PEBS or BTS.

Workaround: Software should always prevent faults on PEBS or BTS.

Status: For the steppings affected, see the *Summary Table of Changes*.



HSM179. Some Memory Performance Monitoring Events May Produce Incorrect Results When Filtering on Either OS or USR Modes

Problem: The memory at-retirement performance monitoring events (listed below) may produce incorrect results when a performance counter is configured in OS-only or USR-only modes (bits 17 or 16 in IA32_PERFVTSELx MSR). Counters with both OS and USR bits set are not affected by this erratum.

Implication: The listed performance monitoring events may produce incorrect results including PEBS records generated at an incorrect point.

The list of affected HSW memory at-retirement events is as follows:

```
MEM_UOPS_RETIRED.STLB_MISS_LOADS event D0H, umask 11H
MEM_UOPS_RETIRED.STLB_MISS_STORES event D0H, umask 12H
MEM_UOPS_RETIRED.LOCK_LOADS event D0H, umask 21H
MEM_UOPS_RETIRED.SPLIT_LOADS event D0H, umask 41H
MEM_UOPS_RETIRED.SPLIT_STORES event D0H, umask 42H
MEM_LOAD_UOPS_RETIRED.L2_HIT event D1H, umask 02H
MEM_LOAD_UOPS_RETIRED.L3_HIT event D1H, umask 04H
MEM_LOAD_UOPS_RETIRED.L1_MISS event D1H, umask 08H
MEM_LOAD_UOPS_RETIRED.L2_MISS event D1H, umask 10H
MEM_LOAD_UOPS_RETIRED.L3_MISS event D1H, umask 20H
MEM_LOAD_UOPS_RETIRED.HIT_LFB event D1H, umask 40H
MEM_LOAD_L3_HIT_RETIRED.XSNP_MISS event D2H, umask 01H
MEM_LOAD_L3_HIT_RETIRED.XSNP_HIT event D2H, umask 02H
MEM_LOAD_L3_HIT_RETIRED.XSNP_HITM event D2H, umask 04H
MEM_LOAD_L3_HIT_RETIRED.XSNP_NONE event D2H, umask 08H
MEM_LOAD_UOPS_L3_MISS_RETIRED.LOCAL_DRAM event D3H, umask 01H
```

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM180. An x87 Store Instruction Which Pends #PE While EPT is Enabled May Lead to an Unexpected Machine Check and/or Incorrect x87 State Information

Problem: The execution of an x87 store instruction which causes a #PE (Precision Exception) to be pended and also causes a VM-exit due to an EPT violation or misconfiguration may lead the VMM logging a machine check exception with a cache hierarchy error (IA32_MCI_STATUS.MCACOD = 0150H and IA32_MCI_STATUS.MSCOD = 000FH). Additionally, FSW.PE and FSW.ES (bits 5 and 7 of the FPU Status Word) may be incorrectly set to 1, and the x87 Last Instruction Opcode (FOP) may be incorrect.

Implication: When this erratum occurs, the VMM may receive an expected machine check exception and software attempting to handle the #PE may not behave as expected.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

**HSM181. Load Latency Performance Monitoring Facility May Stop Counting**

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 (PEBS extension). However due to this erratum, load latency facility may stop counting load instructions when Intel® HyperThreading Technology is enabled.

Implication: Counters programmed with the affected events stop incrementing and do not generate PEBS records.

Workaround: None identified.

Status: For the steppings affected, see *the Summary Table of Changes*.

HSM182. Writing MSR_LASTBRANCH_x_FROM_IP May #GP When Intel® TSX is Not Supported

Problem: Due to this erratum, on processors that do not support Intel TSX (Intel® Transactional Synchronization Extensions) (CPUID.07H.EBX bits 4 and 11 are both zero), writes to MSR_LASTBRANCH_x_FROM_IP (MSR 680H to 68FH) may #GP unless bits [62:61] are equal to bit [47].

Implication: The value read from MSR_LASTBRANCH_x_FROM_IP is unaffected by this erratum; bits [62:61] contain IN_TSX and TSX_ABORT information respectively. Software restoring these MSRs from saved values are subject to this erratum.

Workaround: Before writing MSR_LASTBRANCH_x_FROM_IP, ensure the value being written has bit [47] replicated in bits [62:61]. This is most easily accomplished by sign extending from bit [47] to bits [62:48].

Status: For the steppings affected, see *the Summary Table of Changes*.

HSM183. APIC Timer Interrupt May Not be Generated at The Correct Time In TSC-Deadline Mode

Problem: After writing to the IA32_TSC_ADJUST MSR (3BH), any subsequent write to the IA32_TSC_DEADLINE MSR (6E0H) may incorrectly process the desired deadline. When this erratum occurs, the resulting timer interrupt may be generated at the incorrect time.

Implication: When the local APIC (Advanced Programmable Interrupt Controller) timer is configured for TSC-Deadline mode, a timer interrupt may be generated much earlier than expected or much later than expected. Intel has not observed this erratum with most commercially available software.

Workaround: It is possible for the BIOS to contain a workaround for this erratum.

Status: For the steppings affected, see *the Summary Table of Changes*.

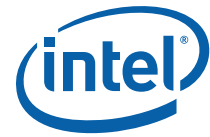
HSM184. System May Hang Under Complex Conditions

Problem: Under complex conditions, insufficient access control in graphics subsystem may lead to a system hang or crash upon a register read.

Implication: When this erratum occurs a system hang or crash may occur.

Workaround: None identified.

Status: For the steppings affected, see *the Summary Table of Changes*.



HSM185. 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=005H with IA32_MCi_STATUS.MSCOD=00FH or IA32_MCi_STATUS.MCACOD=0150H with IA32_MCi_STATUS.MSCOD=00FH) 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 (PA), memory type (PWT, PCD and PAT bits), or User/Supervisor (U/S) bit; 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 (e.g., 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, see the *Summary Table of Changes*.

HSM186. Performance Monitoring General Counter 2 May Have Invalid Value Written When TSX Is Enabled

Problem: When Transactional Synchronization Extensions (TSX) is enabled, and there are aborts (HLE or RTM) overlapping with access or manipulation of the IA32_PMC2 general-purpose performance counter (Offset: C3h) it may return invalid value.

Implication: Software may read invalid value from IA32_PMC2.

Workaround: None identified.

Status: For the steppings affected, see the *Summary Table of Changes*.

HSM187. PMU MSR_UNC_PERF_FIXED_CTR is Cleared After Pkg C7 or Deeper

Problem: The Performance Monitoring Unit Uncore Performance Fixed Counter (MSR_UNC_PERF_FIXED_CTR (MSR 395h)) is cleared after pkg C7 or deeper.

Implication: Due to this erratum, once the system enters pkg C7 or deeper the uncore fixed counter does not reflect the actual count.

Implication: None Identified.

Workaround: For the steppings affected, see the *Summary Table of Changes*.





Specification Changes

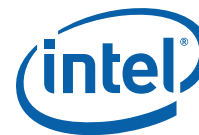
The Specification Changes listed in this section apply to the following documents:

- *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*

HSM1. TSX Instruction

Due to Erratum HSM148, TSX instructions are disabled and are only supported for software development. See your Intel representative for details.

§ §



Specification Clarifications

The Specification Clarifications listed in this section may apply to the following documents:

- *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*

§ §



Documentation Changes

The Documentation Changes listed in this section apply to the following documents:

- *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*

All Documentation Changes will be incorporated into a future version of the appropriate Processor documentation.

Note: Documentation changes for Intel® 64 and IA-32 Architecture Software Developer's Manual volumes 1, 2A, 2B, 3A, and 3B will be posted in a separate document, Intel® 64 and IA-32 Architecture Software Developer's Manual Documentation Changes. Use the following link to become familiar with this file: <http://developer.intel.com/products/processor/manuals/index.htm>

There are no new Documentation Changes in this Specification Update revision.

HSM1. On-Demand Clock Modulation Feature Clarification

Software Controlled Clock Modulation section of the Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B: System Programming Guide will be modified to differentiate On-demand clock modulation feature on different processors. The clarification will state:

For Hyper-Threading Technology enabled processors, the IA32_CLOCK_MODULATION register is duplicated for each logical processor. In order for the On-demand clock modulation feature to work properly, the feature must be enabled on all the logical processors within a physical processor. If the programmed duty cycle is not identical for all the logical processors, the processor clock will modulate to the highest duty cycle



programmed for processors if the CPUID DisplayFamily_DisplayModel signatures is identical for all logical processors in the same core, the processor will modulate at the lowest programmed duty cycle.

For multiple processor cores in a physical package, each core can modulate to a programmed duty cycle independently.

For the P6 family processors, on-demand clock modulation was implemented through the chipset, which controlled clock modulation through the processor's STPCLK# pin.

Table 14-2. CPUID Signatures for Legacy Processors That Resolve to Higher Performance Setting of Conflicting Duty Cycle Requests

Display Family Display Model	Display Family Display Model	Display Family Display Model	Display Family Display Model
0F_xx	06_1C	06_1A	06_1E
06_1F	06_25	06_26	06_27
06_2C	06_2E	06_2F	06_35
06_36			

