

Intel® Core™ i7-900 Desktop Processor Extreme Edition Series and Intel® Core™ i7-900 Desktop Processor Series

Specification Update

March 2012

Notice:

Intel® Core™ i7-900 Desktop Processor Extreme Edition Series and Intel® Core™ i7-900 Desktop Processor Series may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are documented in this Specification Update.



INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document 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.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: <http://www.intel.com/design/literature.htm>.

Code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See http://www.intel.com/products/processor_number for details.

Intel® Core™ i7-900 Desktop Processor Extreme Edition Series and Intel® Core™ i7-900 Desktop Processor Series 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.

The Intel® Core™ i7-900 desktop processor Extreme Edition and Intel® Core™ i7-900 desktop processor 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® 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® Turbo Boost Technology requires a system with Intel® Turbo Boost Technology capability. Consult your PC manufacturer. Performance varies depending on hardware, software and system configuration. For more information, visit <http://www.intel.com/technology/turboboost>.

Enhanced Intel® SpeedStep Technology: See the Processor Spec Finder at <http://ark.intel.com> or contact your Intel representative for more information.

Intel, the Intel logo, Celeron, Pentium, Xeon, Intel SpeedStep, Intel Core, and Core Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Copyright © 2008-2012, Intel Corporation. All rights reserved.



Contents

Preface	6
Summary Tables of Changes	8
Identification Information	17
Errata	19
Specification Changes	75
Specification Clarifications.....	76
Documentation Changes	77



Revision History

Revision	Description	Date
-001	<ul style="list-style-type: none">• Initial Release	November 2008
-002	<ul style="list-style-type: none">• Updated Specification Clarification AAJ1• Added Erratum AAJ89	January 2009
-003	<ul style="list-style-type: none">• Updated Errata AAJ21, AAJ69• Added Errata AAJ90-AAJ105	March 11th 2009
-004	<ul style="list-style-type: none">• Added D0 stepping information• Included i7-920 processor conversion to D0 step• Deleted Erratum AAJ105 and replaced with new erratum• Added Errata AAJ106-AAJ108	May 13th 2009
-005	<ul style="list-style-type: none">• Included Intel® Core™ i7-975 processor Extreme Edition and Intel® Core™ i7-950 processor	June 3rd 2009
-006	<ul style="list-style-type: none">• Added Errata AAJ109 - AAJ117	July 15th 2009
-007	<ul style="list-style-type: none">• Added Errata AAJ118 - AAJ124	Aug 12th 2009
-008	<ul style="list-style-type: none">• Added Errata AAJ125 and AAJ126	September 9th 2009
-009	<ul style="list-style-type: none">• Added Errata AAJ127 - AAJ132	October 12th, 2009
-010	<ul style="list-style-type: none">• Added Intel® Core™ i7-960 information	October 19th, 2009
-011	<ul style="list-style-type: none">• Added Errata AAJ133 - AAJ136	November 9th , 2009
-012	<ul style="list-style-type: none">• Updated Errata AAJ121 and AAJ126	January, 2010
-013	<ul style="list-style-type: none">• Added Errata AAJ137	February 7th, 2010
-014	<ul style="list-style-type: none">• Added Intel® Core™ i7-930 information	February 28th, 2010
-015	<ul style="list-style-type: none">• Added Errata AAJ 138	March 16th, 2010
-016	<ul style="list-style-type: none">• Added Errata AAJ 139	April 13th, 2010
-017	<ul style="list-style-type: none">• Added Errata AAJ 140 and 141	July 19th , 2010



-018	<ul style="list-style-type: none">• Added Errata AAJ142• Updated Erratum AAJ72	October 13th , 2010
-019	<ul style="list-style-type: none">• Added AAJ143	December 8th, 2010
-020	<ul style="list-style-type: none">• • Added Errata AAJ144, AAJ145 and AAJ146• • Updated Erratum AAJ81	January 12th, 2011
-021	<ul style="list-style-type: none">• Added Errata AAJ147, AAJ148, AAJ149, AAJ150, AAJ151• Updated Erratum AAJ45	February 16th, 2011
-022	<ul style="list-style-type: none">• Added Errata AAJ152 and AAJ153	May 18th, 2011
-023	<ul style="list-style-type: none">• Added Erratum AAJ154	August 17th, 2011
-024	<ul style="list-style-type: none">• Added Erratum AAJ155	September 14 th , 2011
-025	<ul style="list-style-type: none">• Updated Erratum AAJ144	October 19 th , 2011
-026	<ul style="list-style-type: none">• Added Erratum AAJ156	March 14 th , 2011

§ §



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 the Nomenclature section 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/Location
<i>Intel® Core™ i7-900 Desktop Processor Extreme Edition Series and Intel® Core™ i7-900 Desktop Processor Series Datasheet Volume 1</i>	http://download.intel.com/design/processor/datashts/320834.pdf
<i>Intel® Core™ i7-900 Desktop Processor Extreme Edition Series and Intel® Core™ i7-900 Desktop Processor Series Datasheet Volume 2</i>	http://download.intel.com/design/processor/datashts/320835.pdf

Related Documents

Document Title	Document Number/Location
<i>AP-485, Intel® Processor Identification and the CPUID Instruction</i>	http://www.intel.com/design/processor/applnots/241618.htm
<i>Intel® 64 and IA-32 Architectures Software Developer's Manual Documentation Changes</i>	http://www.intel.com/design/processor/specupdt/252046.htm
<i>ACPI Specifications</i>	www.acpi.info
<i>Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1: Basic Architecture</i> <i>Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A: Instruction Set Reference Manual A-M</i> <i>Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2B: Instruction Set Reference Manual N-Z</i> <i>Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A: System Programming Guide</i> <i>Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B: System Programming Guide</i> <i>Intel® 64 and IA-32 Intel Architecture Optimization Reference Manual</i>	http://www.intel.com/products/processor/manuals/index.htm



Nomenclature

Errata are design defects or errors. These may cause the Intel® Core™ i7 processor Extreme Edition and Intel® Core™ i7 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, e.g., 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, etc).





Summary Tables of Changes

The following tables indicate the errata, specification changes, specification clarifications, or documentation changes which apply to the Intel® Core™ i7 processor Extreme Edition and Intel® Core™ i7 Desktop processor product. 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

Shaded:	This item is either new or modified from the previous version of the document.
---------	--

Each Specification Update item is prefixed with a capital letter to distinguish the product. The key below details the letters that are used in Intel's microprocessor Specification Updates:



No	C-0	D-0	Status	ERRATA
AAJ1	X	X	No Fix	MCI_Status Overflow Bit May Be Incorrectly Set on a Single Instance of a DTLB Error
AAJ2	X	X	No Fix	Debug Exception Flags DR6.B0-B3 Flags May be Incorrect for Disabled Breakpoints
AAJ3	X	X	No Fix	MONITOR or CLFLUSH on the Local XAPIC's Address Space Results in Hang
AAJ4	X	X	No Fix	Corruption of CS Segment Register During RSM While Transitioning From Real Mode to Protected Mode
AAJ5	X	X	No Fix	The Processor May Report a #TS Instead of a #GP Fault
AAJ6	X	X	No Fix	REP MOVS/STOS Executing with Fast Strings Enabled and Crossing Page Boundaries with Inconsistent Memory Types may use an Incorrect Data Size or Lead to Memory-Ordering Violations
AAJ7	X	X	No Fix	Code Segment Limit/Canonical Faults on RSM May be Serviced before Higher Priority Interrupts/Exceptions and May Push the Wrong Address Onto the Stack
AAJ8	X	X	No Fix	Performance Monitor SSE Retired Instructions May Return Incorrect Values
AAJ9	X	X	No Fix	Premature Execution of a Load Operation Prior to Exception Handler Invocation
AAJ10	X	X	No Fix	MOV To/From Debug Registers Causes Debug Exception
AAJ11	X	X	No Fix	Incorrect Address Computed For Last Byte of FXSAVE/FXRSTOR Image Leads to Partial Memory Update
AAJ12	X	X	No Fix	Values for LBR/BTS/BTM will be Incorrect after an Exit from SMM
AAJ13	X	X	No Fix	Single Step Interrupts with Floating Point Exception Pending May Be Mishandled
AAJ14	X	X	No Fix	Fault on ENTER Instruction May Result in Unexpected Values on Stack Frame
AAJ15	X	X	No Fix	IRET under Certain Conditions May Cause an Unexpected Alignment Check Exception
AAJ16	X	X	No Fix	General Protection Fault (#GP) for Instructions Greater than 15 Bytes May be Preempted
AAJ17	X	X	No Fix	General Protection (#GP) Fault May Not Be Signaled on Data Segment Limit Violation above 4-G Limit
AAJ18	X	X	No Fix	LBR, BTS, BTM May Report a Wrong Address when an Exception/Interrupt Occurs in 64-bit Mode
AAJ19	X	X	No Fix	Performance Monitoring Events for Read Miss to Level 3 Cache Fill Occupancy Counter may be Incorrect
AAJ20	X	X	No Fix	A VM Exit on MWAIT May Incorrectly Report the Monitoring Hardware as Armed
AAJ21	X	X	No Fix	Memory Aliasing of Code Pages May Cause Unpredictable System Behavior
AAJ22	X	X	No Fix	Delivery Status of the LINT0 Register of the Local Vector Table May be Lost



No	C-0	D-0	Status	ERRATA
AAJ23	X	X	No Fix	Performance Monitor Event SEGMENT_REG_LOADS Counts Inaccurately
AAJ24	X	X	No Fix	#GP on Segment Selector Descriptor that Straddles Canonical Boundary May Not Provide Correct Exception Error Code
AAJ25	X	X	No Fix	Improper Parity Error Signaled in the IQ Following Reset When a Code Breakpoint is Set on a #GP Instruction
AAJ26	X	X	No Fix	An Enabled Debug Breakpoint or Single Step Trap May Be Taken after MOV SS/POP SS Instruction if it is Followed by an Instruction That Signals a Floating Point Exception
AAJ27	X	X	No Fix	IA32_MPERF Counter Stops Counting During On-Demand TM1
AAJ28	X	X	No Fix	Intel® QuickPath Memory Controller tTHROT_OPREF Timings May be Violated During Self Refresh Entry
AAJ29	X	X	No Fix	Processor May Over Count Correctable Cache MESI State Errors
AAJ30	X	X	No Fix	Synchronous Reset of IA32_APERF/IA32_MPERF Counters on Overflow Does Not Work
AAJ31	X	X	No Fix	Disabling Thermal Monitor While Processor is Hot, Then Re-enabling, May Result in Stuck Core Operating Ratio
AAJ32	X		Fixed	The PECC Throttling Counter May Not be Accurate
AAJ33	X	X	No Fix	PECC Does Not Support PCI Configuration Reads/Writes to Misaligned Addresses
AAJ34	X	X	No Fix	OVER Bit for IA32_MCI_STATUS Register May Get Set on Specific Internal Error
AAJ35	X	X	No Fix	Writing the Local Vector Table (LVT) when an Interrupt is Pending May Cause an Unexpected Interrupt
AAJ36	X		Fixed	A Processor Core May Not Wake Up from S1 State
AAJ37	X	X	No Fix	Reading Reserved APIC Registers May Not Signal an APIC Error
AAJ38	X		Fixed	A Logical Processor Receiving a SIPI After a VM Entry Into WFS State May Become Unresponsive
AAJ39	X	X	No Fix	Memory Controller May Deliver Incorrect Data When Memory Ranks Are In Power-Down
AAJ40	X	X	No Fix	Faulting MMX Instruction May Incorrectly Update x87 FPU Tag Word
AAJ41	X		Fixed	A Floating-Point Store Instruction May Cause an Unexpected x87 FPU Floating-Point Error (#MF)
AAJ42	X		Fixed	Incorrect TLB Translation May Occur After Exit From C6
AAJ43	X		Fixed	USB 1.1 ISOCH Audio Glitches with Intel® QuickPath Interconnect Locks and Deep C-States
AAJ44	X		Fixed	Stack Pointer May Become Incorrect In Loops With Unbalanced Push and Pop Operations
AAJ45	X		No Fix	A P-state Change While Another Core is in C6 May Prevent Further C-state and P-state Transitions



No	C-0	D-0	Status	ERRATA
AAJ46	X	X	No Fix	Certain Store Parity Errors May Not Log Correct Address in IA32_MCI_ADDR
AAJ47	X	X	No Fix	xAPIC Timer May Decrement Too Quickly Following an Automatic Reload While in Periodic Mode
AAJ48	X	X	No Fix	Certain Undefined Opcodes Crossing a Segment Limit May Result in #UD Instead of #GP Exception
AAJ49	X	X	No Fix	Indication of A20M Support is Inverted
AAJ50	X	X	No Fix	Reported Memory Type May Not Be Used to Access the VMCS and Referenced Data Structures
AAJ51	X		Fixed	After VM Entry, Instructions May Incorrectly Operate as if CS.D=0
AAJ52	X		Fixed	Spurious Machine Check Error May Occur When Logical Processor is Woken Up
AAJ53	X	X	No Fix	B0-B3 Bits in DR6 For Non-Enabled Breakpoints May be Incorrectly Set
AAJ54	X	X	No Fix	Core C6 May Clear Previously Logged TLB Errors
AAJ55	X	X	No Fix	Processor May Hang When Two Logical Processors Are in Specific Low Power States
AAJ56	X	X	No Fix	MOVNTDQA From WC Memory May Pass Earlier Locked Instructions
AAJ57	X	X	No Fix	Performance Monitor Event MISALIGN_MEM_REF May Over Count
AAJ58	X	X	No Fix	Changing the Memory Type for an In-Use Page Translation May Lead to Memory-Ordering Violations
AAJ59	X		Fixed	Writes to IA32_CR_PAT or IA32_EFER MSR May Cause an Incorrect ITLB Translation
AAJ60	X		Fixed	The "Virtualize APIC Accesses" VM-Execution Control May be Ignored
AAJ61	X		Fixed	C6 Transitions May Cause Spurious Updates to the xAPIC Error Status Register
AAJ62	X		Fixed	Critical ISOCH Traffic May Cause Unpredictable System Behavior When Write Major Mode Enabled
AAJ63	X	X	No Fix	Running with Write Major Mode Disabled May Lead to a System Hang
AAJ64	X	X	No Fix	Memory Controller Address Parity Error Injection Does Not Work Correctly
AAJ65	X	X	No Fix	Memory Controller Opportunistic Refreshes Might be Missed
AAJ66	X	X	No Fix	Delivery of Certain Events Immediately Following a VM Exit May Push a Corrupted RIP Onto The Stack
AAJ67	X	X	No Fix	The Combination of a Bus Lock and a Data Access That is Split Across Page Boundaries May Lead to Processor Livelock
AAJ68	X	X	No Fix	CPUID Instruction Returns Incorrect Brand String
AAJ69	X	X	No Fix	An Unexpected Page Fault May Occur Following the Unmapping and Re-mapping of a Page



No	C-0	D-0	Status	ERRATA
AAJ70	X	X	No Fix	Infinite Stream of Interrupts May Occur if an ExtINT Delivery Mode Interrupt is Received while All Cores in C6
AAJ71	X	X	No Fix	Two xAPIC Timer Event Interrupts May Unexpectedly Occur
AAJ72	X	X	No Fix	EOI Transaction May Not be Sent if Software Enters Core C6 During an Interrupt Service Routine
AAJ73	X	X	No Fix	FREEZE_WHILE_SMM Does Not Prevent Event From Pending PEBS During SMM
AAJ74	X	X	No Fix	PEBS Records For Load Latency Monitoring May Contain an Incorrect Linear Address
AAJ75	X	X	No Fix	PEBS Field "Data Linear Address" is Not Sign Extended to 64 Bits
AAJ76	X	X	No Fix	Core C6 May Not Operate Correctly in the Presence of Bus Locks
AAJ77	X	X	No Fix	Intel® Turbo Boost Technology May be Limited Immediately After Package C-state Exit with QPI L1 Mode Disabled
AAJ78	X	X	No Fix	APIC Error "Received Illegal Vector" May be Lost
AAJ79	X	X	No Fix	CPUID Incorrectly Indicates the UnHalted Reference Cycle Architectural Event is Supported
AAJ80	X		Fixed	Architectural Performance Monitor Event 'Branch Misses Retired' is Counted Incorrectly
AAJ81	X	X	No Fix	DR6.B0-B3 May Not Report All Breakpoints Matched When a MOV/POP SS is Followed by a Store Instruction
AAJ82	X	X	No Fix	An Uncorrectable Error Logged in IA32_CR_MC2_STATUS May also Result in a System Hang
AAJ83	X	X	No Fix	IA32_PERF_GLOBAL_CTRL MSR May be Incorrectly Initialized
AAJ84	X	X	No Fix	Performance Monitor Interrupts Generated From Uncore Fixed Counters (394H) May be Ignored
AAJ85	X	X	No Fix	Processors with SMT May Hang on P-State Transition or ACPI Clock Modulation Throttling
AAJ86	X	X	No Fix	Performance Monitor Counter INST_RETIRED.STORES May Count Higher than Expected
AAJ87	X	X	No Fix	Sleeping Cores May Not be Woken Up on Logical Cluster Mode Broadcast IPI Using Destination Field Instead of Shorthand
AAJ88	X	X	No Fix	Faulting Executions of FXRSTOR May Update State Inconsistently
AAJ89	X	X	No Fix	Unexpected QPI Link Behavior May Occur When a CRC Error Happens During L0s
AAJ90	X	X	No Fix	Performance Monitor Event EPT.EPDPE_MISS May be Counted While EPT is Disabled
AAJ91	X	X	No Fix	Performance Monitor Counters May Count Incorrectly
AAJ92	X	X	No Fix	Processor Forward Progress Mechanism Interacting With Certain MSR/CSR Writes May Cause Unpredictable System Behavior
AAJ93	X		Fixed	USB 1.1 Isoch Memory Latencies May Increase During Package C3/C6 Transitions



No	C-0	D-0	Status	ERRATA
AAJ94	X	X	No Fix	Processor May Incorrectly Demote Processor C6 State to a C3 State
AAJ95	X	X	No Fix	Performance Monitor Event Offcore_response_0 (B7H) Does Not Count NT Stores to Local DRAM Correctly
AAJ96	X	X	No Fix	EFLAGS Discrepancy on Page Faults and on EPT-Induced VM Exits after a Translation Change
AAJ97	X	X	No Fix	System May Hang if MC_CHANNEL_{0,1,2}_MC_DIMM_INIT_CMD.DO_ZQCL Commands Are Not Issued in Increasing Populated DDR3 Rank Order
AAJ98	X	X	No Fix	LER and LBR MSRs May Be Incorrectly Updated During a Task Switch
AAJ99	X		Fixed	Virtualized WRMSR to the IA32_EXT_XAPIC_TPR MSR Uses Incorrect Value for TPR Threshold
AAJ100	X	X	No Fix	Back to Back Uncorrected Machine Check Errors May Overwrite IA32_MC3_STATUS.MSCOD
AAJ101	X	X	No Fix	Memory Intensive Workloads with Core C6 Transitions May Cause System Hang
AAJ102	X	X	No Fix	Corrected Errors With a Yellow Error Indication May be Overwritten by Other Corrected Errors
AAJ103	X	X	No Fix	PSI# Signal May Incorrectly be Left Asserted
AAJ104	X	X	No Fix	A String Instruction that Re-maps a Page May Encounter an Unexpected Page Fault
AAJ105	X	X	No Fix	Performance Monitor Events DCACHE_CACHE_LD and DCACHE_CACHE_ST May Overcount
AAJ106	X	X	No Fix	Rapid Core C3/C6 Transition May Cause Unpredictable System Behavior
AAJ107	X	X	No Fix	Performance Monitor Events INSTR_RETIRED and MEM_INST_RETIRED May Count Inaccurately
AAJ108	X	X	No Fix	A Page Fault May Not be Generated When the PS bit is set to "1" in a PML4E or PDPTE
AAJ109	X	X	Plan Fix	tRP Timing Violations May be Observed Near a Self Refresh Entry
AAJ110	X	X	No Fix	System May Hang if MC_CHANNEL_{0,1,2}_MC_DIMM_INIT_CMD.DO_ZQCL Commands Are Not Issued in Increasing Populated DDR3 Rank Order
AAJ111	X	X	No Fix	Concurrent Updates to a Segment Descriptor May be Lost
AAJ112	X	X	No Fix	Memory Controller Clock Circuits May Show a Temperature Sensitive Dependence on Power-On Conditions
AAJ113	X	X	No Fix	PMIs May be Lost During Core C6 Transitions
AAJ114	X	X	No Fix	Uncacheable Access to a Monitored Address Range May Prevent Future Triggering of the Monitor Hardware
AAJ115	X	X	No Fix	BIST Results May be Additionally Reported After a GETSEC[WAKEUP] or INIT-SIPI Sequence



No	C-0	D-0	Status	ERRATA
AAJ116	X	X	No Fix	Pending x87 FPU Exceptions (#MF) May be Signaled Earlier Than Expected
AAJ117	X	X	No Fix	VM Exits Due to "NMI-Window Exiting" May Be Delayed by One Instruction
AAJ118	X	X	No Fix	VM Exits Due to EPT Violations Do Not Record Information About Pre-IRET NMI Blocking
AAJ119	X	X	No Fix	Multiple Performance Monitor Interrupts are Possible on Overflow of IA32_FIXED_CTR2
AAJ120	X	X	No Fix	LBRs May Not be Initialized During Power-On Reset of the Processor
AAJ121	X	X	No Fix	Unexpected Interrupts May Occur on C6 Exit If Using APIC Timer to Generate Interrupts
AAJ122	X	X	No Fix	LBR, BTM or BTS Records May have Incorrect Branch From Information After an EIST Transition, T-states, C1E, or Adaptive Thermal Throttling
AAJ123	X	X	No Fix	Redirection to Probe Mode May be delayed beyond Intended Instruction
AAJ124	X	X	No Fix	VMX-Preemption Timer Does Not Count Down at the Rate Specified
AAJ125	X	X	No Fix	Multiple Performance Monitor Interrupts are Possible on Overflow of Fixed Counter 0
AAJ126	X	X	No Fix	VM Exits Due to LIDT/LGDT/SIDT/SGDT Do Not Report Operand Size
AAJ127	X		No Fix	Performance Monitoring Events STORE_BLOCKS.NOT_STA and STORE_BLOCKS.STA May Not Count Events Correctly
AAJ128	X	X	No Fix	Storage of PEBS Record Delayed Following Execution of MOV SS or STI
AAJ129	X	X	No Fix	Performance Monitoring Event FP_MMX_TRANS_TO_MMX May Not Count Some Transitions
AAJ130	X	X	Plan Fix	INVLPG Following INVEPT or INVVPID May Fail to Flush All Translations for a Large Page
AAJ131	X	X	No Fix	The PECCI Bus May be Tri-stated After System Reset
AAJ132	X	X	No Fix	LER MSRs May Be Unreliable
AAJ133	X	X	No Fix	An Exit From the Core C6-state May Result in the Dropping of an Interrupt
AAJ134	X	X	No Fix	PMIs During Core C6 Transitions May Cause the System to Hang
AAJ135	X	X	No Fix	2MB Page Split Lock Accesses Combined With Complex Internal Events May Cause Unpredictable System Behavior
AAJ136	X	X	No Fix	IA32_MC8_CTL2 MSR is Not Cleared on Processor Warm Reset
AAJ137	X	X	No Fix	The Combination of a Page-Split Lock Access And Data Accesses That Are Split Across Cacheline Boundaries May Lead to Processor Livelock



No	C-0	D-0	Status	ERRATA
AAJ138	X	X	No Fix	FP Data Operand Pointer May Be Incorrectly Calculated After an FP Access Which Wraps a 4-Gbyte Boundary in Code That Uses 32-Bit Address Size in 64-bit Mode
AAJ139	X	X	No Fix	IO_SMI Indication in SMRAM State Save Area May Be Lost
AAJ140	X	X	No Fix	Performance Monitor Events for Hardware Prefetches Which Miss The L1 Data Cache May be Over Counted
AAJ141	X	X	No Fix	VM Exit May Incorrectly Clear IA32_PERF_GLOBAL_CTRL [34:32]
AAJ142	X	X	No Fix	QPI Lane May Be Dropped During Full Frequency Deskew Phase of Training
AAJ143	X	X	No Fix	PerfMon Overflow Status Can Not be Cleared After Certain Conditions Have Occurred
AAJ144	X	X	No Fix	An Unexpected Page Fault or EPT Violation May Occur After Another Logical Processor Creates a Valid Translation for a Page
AAJ145	X	X	No Fix	L1 Data Cache Errors May be Logged With Level Set to 1 Instead of 0
AAJ146	X	X	No Fix	Stack Pushes May Not Occur Properly for Events Delivered Immediately After VM Entry to 16-Bit Software
AAJ147	X	X	No Fix	PerfMon Event LOAD_HIT_PRE.SW_PREFETCH May Overcount
AAJ148	X	X	No Fix	Successive Fixed Counter Overflows May be Discarded
AAJ149	X	X	No Fix	#GP May be Signaled When Invalid VEX Prefix Precedes Conditional Branch Instructions
AAJ150	X	X	No Fix	A Logical Processor May Wake From Shutdown State When Branch-Trace Messages or Branch-Trace Stores Are Enabled
AAJ151	X	X	No Fix	Task Switch to a TSS With an Inaccessible LDTR Descriptor May Cause Unexpected Faults
AAJ152	X	X	No Fix	Changes to Reserved Bits of Some Non-Architectural MSR's May Cause Unpredictable System Behavior
AAJ153	X	X	No Fix	VM Entries That Return From SMM Using VMLAUNCH May Not Update The Launch State of the VMCS
AAJ154	X	X	No Fix	VM Entry May Clear Bytes 81H-83H on Virtual-APIC Page When "Use TPR Shadow" Is 0
AAJ155	X	X	No Fix	A First Level Data Cache Parity Error May Result in Unexpected Behavior
AAJ156	X	X	No Fix	An Event May Intervene Before a System Management Interrupt That Results from IN or INS



No	SPECIFICATION CHANGES
-	There are no Specification Changes in this Specification Update revision.

No	SPECIFICATION CLARIFICATIONS
AAJ1	Clarification of TRANSLATION LOOKASIDE BUFFERS (TLBS) Invalidation.

No	DOCUMENTATION CHANGES
-	There are no Documentation Changes in this Specification Update revision.

§ §



Identification Information

Component Identification via Programming Interface

The Intel® Core™ i7 processor Extreme Edition and Intel® Core™ i7 processor stepping can be identified by the following register contents:

Reserved	Extended Family ¹	Extended Model ²	Reserved	Processor Type ³	Family Code ⁴	Model Number ⁵	Stepping ID ⁶
31:28	27:20	19:16	15:14	13:12	11:8	7:4	3:0
	00000000b	0001b		00b	0110	1010b	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 Pro, Pentium 4, Intel® Core™ processor family or Intel® Core i7 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 Processor Type, specified in bits [13:12] indicates whether the processor is an original OEM processor, an OverDrive processor, or a dual processor (capable of being used in a dual processor system).
4. 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.
5. 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.
6. The Stepping ID in bits [3:0] indicates the revision number of that model. See Table 1 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.



Component Marking Information

The Intel® Core™ i7 processor Extreme Edition and Intel® Core™ i7 processor stepping can be identified by the following component markings:

Figure 1. Processor Top-side Markings (Example)

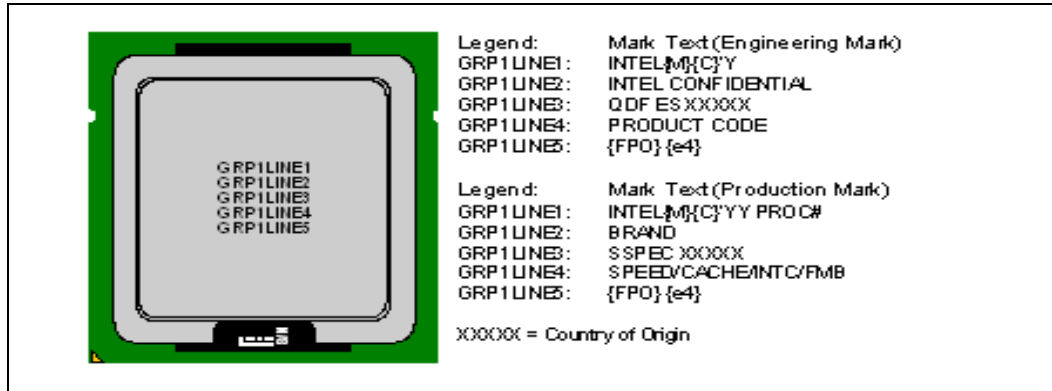


Table 1. Intel® Core™ i7 Processor Extreme Edition and Intel® Core™ i7 Processor Identification

QDF/S-Spec	Stepping	Processor Number	Processor Signature	Core Frequency (GHz) / Intel QuickPath Interconnect (GT/s) / DDR3 (MHz)	Available bins of Intel® Turbo Boost Technology ²	Cache Size (MB)	Notes
SLBCJ	C-0	i7-965	0x000106A4	3.20 / 6.40/ 1066	1/1/1/2	8	1
SLBCK	C-0	i7-940	0x000106A4	2.93 / 4.80/ 1066	1/1/1/2	8	
SLBCH	C-0	i7-920	0x000106A4	2.66 / 4.80/ 1066	1/1/1/2	8	
SLBEQ	D-0	i7-975	0x000106A5	3.33 / 6.40/ 1066	1/1/1/2	8	1
SLBEU	D-0	i7-960	0x000106A5	3.20 / 4.80/ 1066	1/1/1/2	8	
SLBEN	D-0	i7-950	0x000106A5	3.06 / 4.80/ 1066	1/1/1/2	8	
SLBKP	D-0	i7-930	0x000106A5	2.80 / 4.80/ 1066	1/1/1/2	8	
SLBEJ	D-0	i7-920	0x000106A5	2.66 / 4.80/ 1066	1/1/1/2	8	

NOTES:

1. Although these units are factory-configured for 1333 MHz integrated memory controller frequency, Intel does not support operation beyond 1066 MHz; however, this processor has additional support to override the integrated memory controller frequency.
2. Column indicates the number of frequency bins (133.33 MHz) of Intel® Turbo Boost Technology that are available for 4, 3, 2, or 1 cores active respectively.





Errata

AAJ1. 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.

AAJ2. Debug Exception Flags DR6.B0-B3 Flags May be Incorrect for Disabled Breakpoints

Problem: When a debug exception is signaled on a load that crosses cache lines with data forwarded from a store and whose corresponding breakpoint enable flags are disabled (DR7.G0-G3 and DR7.L0-L3), the DR6.B0-B3 flags may be incorrect.

Implication: The debug exception DR6.B0-B3 flags may be incorrect for the load if the corresponding breakpoint enable flag in DR7 is disabled.

Workaround: None identified.

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

AAJ3. 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.

**AAJ4. Corruption of CS Segment Register during RSM While Transitioning From Real Mode to Protected Mode**

Problem: During the transition from real mode to protected mode, if an SMI (System Management Interrupt) occurs between the MOV to CR0 that sets PE (Protection Enable, bit 0) and the first FAR JMP, the subsequent RSM (Resume from System Management Mode) may cause the lower two bits of CS segment register to be corrupted.

Implication: The corruption of the bottom two bits of the CS segment register will have no impact unless software explicitly examines the CS segment register between enabling protected mode and the first FAR JMP. *Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 3A: System Programming Guide, Part 1*, in the section titled "Switching to Protected Mode" recommends the FAR JMP immediately follows the write to CR0 to enable protected mode. 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.

AAJ5. The Processor May Report a #TS Instead of a #GP Fault

Problem: A jump to a busy TSS (Task-State Segment) may cause a #TS (invalid TSS exception) instead of a #GP fault (general protection exception).

Implication: Operation systems that access a busy TSS may get invalid TSS fault instead of a #GP fault. 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.



AAJ6. REP MOVS/STOS Executing with Fast Strings Enabled and Crossing Page Boundaries with Inconsistent Memory Types may use an Incorrect Data Size or Lead to Memory-Ordering Violations

Problem: Under certain conditions as described in the Software Developers Manual section "Out-of-Order Stores For String Operations in Pentium 4, Intel Xeon, and P6 Family Processors" the processor performs REP MOVS or REP STOS as fast strings. Due to this erratum fast string REP MOVS/REP STOS instructions that cross page boundaries from WB/WC memory types to UC/WP/WT memory types, may start using an incorrect data size or may observe memory ordering violations.

Implication: Upon crossing the page boundary the following may occur, dependent on the new page memory type:

- UC the data size of each write will now always be 8 bytes, as opposed to the original data size.
- WP the data size of each write will now always be 8 bytes, as opposed to the original data size and there may be a memory ordering violation.
- WT there may be a memory ordering violation.

Workaround: Software should avoid crossing page boundaries from WB or WC memory type to UC, WP or WT memory type within a single REP MOVS or REP STOS instruction that will execute with fast strings enabled.

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

AAJ7. Code Segment Limit/Canonical Faults on RSM May be Serviced before Higher Priority Interrupts/Exceptions and May Push the Wrong Address Onto the Stack

Problem: Normally, when the processor encounters a Segment Limit or Canonical Fault due to code execution, a #GP (General Protection Exception) fault is generated after all higher priority Interrupts and exceptions are serviced. Due to this erratum, if RSM (Resume from System Management Mode) returns to execution flow that results in a Code Segment Limit or Canonical Fault, the #GP fault may be serviced before a higher priority Interrupt or Exception (e.g. NMI (Non-Maskable Interrupt), Debug break(#DB), Machine Check (#MC), etc.). If the RSM attempts to return to a non-canonical address, the address pushed onto the stack for this #GP fault may not match the non-canonical address that caused the fault.

Implication: Operating systems may observe a #GP fault being serviced before higher priority Interrupts and Exceptions. Intel has not observed this erratum on any commercially available software.

Workaround: None identified.

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

**AAJ8. Performance Monitor SSE Retired Instructions May Return Incorrect Values**

Problem: Performance Monitoring counter SIMD_INST_RETIRED (Event: C7H) is used to track retired SSE instructions. Due to this erratum, the processor may also count other types of instructions resulting in higher than expected values.

Implication: Performance Monitoring counter SIMD_INST_RETIRED may report count higher than expected.

Workaround: None identified.

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

AAJ9. Premature Execution of a Load Operation Prior to Exception Handler Invocation

Problem: If any of the below circumstances occur, it is possible that the load portion of the instruction will have executed before the exception handler is entered.

- If an instruction that performs a memory load causes a code segment limit violation.
- If a waiting X87 floating-point (FP) instruction or MMX™ technology (MMX) instruction that performs a memory load has a floating-point exception pending.
- If an MMX or SSE/SSE2/SSE3/SSSE3 extensions (SSE) instruction that performs a memory load and has either CR0.EM=1 (Emulation bit set), or a floating-point Top-of-Stack (FP TOS) not equal to 0, or a DNA exception pending.

Implication: In normal code execution where the target of the load operation is to write back memory there is no impact from the load being prematurely executed, or from the restart and subsequent re-execution of that instruction by the exception handler. If the target of the load is to uncached memory that has a system side-effect, restarting the instruction may cause unexpected system behavior due to the repetition of the side-effect. Particularly, while CR0.TS [bit 3] is set, a MOVD/MOVQ with MMX/XMM register operands may issue a memory load before getting the DNA exception.

Workaround: Code which performs loads from memory that has side-effects can effectively workaround this behavior by using simple integer-based load instructions when accessing side-effect memory and by ensuring that all code is written such that a code segment limit violation cannot occur as a part of reading from side-effect memory.

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

**AAJ10. MOV To/From Debug Registers Causes Debug Exception**

Problem: When in V86 mode, if a MOV instruction is executed to/from a debug registers, a general-protection exception (#GP) should be generated. However, in the case when the general detect enable flag (GD) bit is set, the observed behavior is that a debug exception (#DB) is generated instead.

Implication: With debug-register protection enabled (i.e., the GD bit set), when attempting to execute a MOV on debug registers in V86 mode, a debug exception will be generated instead of the expected general-protection fault.

Workaround: In general, operating systems do not set the GD bit when they are in V86 mode. The GD bit is generally set and used by debuggers. The debug exception handler should check that the exception did not occur in V86 mode before continuing. If the exception did occur in V86 mode, the exception may be directed to the general-protection exception handler.

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

AAJ11. Incorrect Address Computed For Last Byte of FXSAVE/FXRSTOR Image Leads to Partial Memory Update

Problem: A partial memory state save of the 512-byte FXSAVE image or a partial memory state restore of the FXRSTOR image may occur if a memory address exceeds the 64KB limit while the processor is operating in 16-bit mode or if a memory address exceeds the 4GB limit while the processor is operating in 32-bit mode.

Implication: FXSAVE/FXRSTOR will incur a #GP fault due to the memory limit violation as expected but the memory state may be only partially saved or restored.

Workaround: Software should avoid memory accesses that wrap around the respective 16-bit and 32-bit mode memory limits.

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

AAJ12. Values for LBR/BTS/BTM will be Incorrect after an Exit from SMM

Problem: After a return from SMM (System Management Mode), the CPU will incorrectly update the LBR (Last Branch Record) and the BTS (Branch Trace Store), hence rendering their data invalid. The corresponding data if sent out as a BTM on the system bus will also be incorrect.

Note: This issue would only occur when one of the 3 above mentioned debug support facilities are used.

Implication: The value of the LBR, BTS, and BTM immediately after an RSM operation should not be used.

Workaround: None identified.

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

**AAJ13. Single Step Interrupts with Floating Point Exception Pending May Be Mishandled**

Problem: In certain circumstances, when a floating point exception (#MF) is pending during single-step execution, processing of the single-step debug exception (#DB) may be mishandled.

Implication: When this erratum occurs, #DB will be incorrectly handled as follows:

- #DB is signaled before the pending higher priority #MF (Interrupt 16)
- #DB is generated twice on the same instruction

Workaround: None identified.

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

AAJ14. Fault on ENTER Instruction May Result in Unexpected Values on Stack Frame

Problem: The ENTER instruction is used to create a procedure stack frame. Due to this erratum, if execution of the ENTER instruction results in a fault, the dynamic storage area of the resultant stack frame may contain unexpected values (i.e. residual stack data as a result of processing the fault).

Implication: Data in the created stack frame may be altered following a fault on the ENTER instruction. Please refer to "Procedure Calls For Block-Structured Languages" in *IA-32 Intel® Architecture Software Developer's Manual, Vol. 1, Basic Architecture*, for information on the usage of the ENTER instructions. This erratum is not expected to occur in ring 3. Faults are usually processed in ring 0 and stack switch occurs when transferring to ring 0. Intel has not observed this erratum on any commercially available software.

Workaround: None identified.

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

AAJ15. IRET under Certain Conditions May Cause an Unexpected Alignment Check Exception

Problem: In IA-32e mode, it is possible to get an Alignment Check Exception (#AC) on the IRET instruction even though alignment checks were disabled at the start of the IRET. This can only occur if the IRET instruction is returning from CPL3 code to CPL3 code. IRETs from CPL0/1/2 are not affected. This erratum can occur if the EFLAGS value on the stack has the AC flag set, and the interrupt handler's stack is misaligned. In IA-32e mode, RSP is aligned to a 16-byte boundary before pushing the stack frame.

Implication: In IA-32e mode, under the conditions given above, an IRET can get a #AC even if alignment checks are disabled at the start of the IRET. This erratum can only be observed with a software generated stack frame.

Workaround: Software should not generate misaligned stack frames for use with IRET.

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

**AAJ16. General Protection Fault (#GP) for Instructions Greater than 15 Bytes May be Preempted**

Problem: When the processor encounters an instruction that is greater than 15 bytes in length, a #GP is signaled when the instruction is decoded. Under some circumstances, the #GP fault may be preempted by another lower priority fault (e.g. Page Fault (#PF)). However, if the preempting lower priority faults are resolved by the operating system and the instruction retried, a #GP fault will occur.

Implication: Software may observe a lower-priority fault occurring before or in lieu of a #GP fault. Instructions of greater than 15 bytes in length can only occur if redundant prefixes are placed before the instruction.

Workaround: None identified.

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

AAJ17. General Protection (#GP) Fault May Not Be Signaled on Data Segment Limit Violation above 4-G Limit

Problem: In 32-bit mode, memory accesses to flat data segments (base = 00000000h) that occur above the 4G limit (0fffffffh) may not signal a #GP fault.

Implication: When such memory accesses occur in 32-bit mode, the system may not issue a #GP fault.

Workaround: Software should ensure that memory accesses in 32-bit mode do not occur above the 4G limit (0fffffffh).

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

AAJ18. 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.

**AAJ19. Performance Monitoring Events for Read Miss to Level 3 Cache Fill Occupancy Counter may be Incorrect**

Problem: Whenever an Level 3 cache fill conflicts with another request's address, the miss to fill occupancy counter, UNC_GQ_ALLOC.RT_LLC_MISS (Event 02H), will provide erroneous results.

Implication: The Performance Monitoring UNC_GQ_ALLOC.RT_LLC_MISS event may count a value higher than expected. The extent to which the value is higher than expected is determined by the frequency of the L3 address conflict.

Workaround: None identified.

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

AAJ20. A VM Exit on MWAIT May Incorrectly Report the Monitoring Hardware as Armed

Problem: A processor write to the address range armed by the MONITOR instruction may not immediately trigger the monitoring hardware. Consequently, a VM exit on a later MWAIT may incorrectly report the monitoring hardware as armed, when it should be reported as unarmed due to the write occurring prior to the MWAIT.

Implication: If a write to the range armed by the MONITOR instruction occurs between the MONITOR and the MWAIT, the MWAIT instruction may start executing before the monitoring hardware is triggered. If the MWAIT instruction causes a VM exit, this could cause its exit qualification to incorrectly report 0x1. In the recommended usage model for MONITOR/MWAIT, there is no write to the range armed by the MONITOR instruction between the MONITOR and the MWAIT.

Workaround: Software should never write to the address range armed by the MONITOR instruction between the MONITOR and the subsequent MWAIT.

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

**AAJ21. Memory Aliasing of Code Pages May Cause Unpredictable System Behavior**

Problem: The type of memory aliasing contributing to this erratum is the case where two different logical processors have the same code page mapped with two different memory types. Specifically, if one code page is mapped by one logical processor as write-back and by another as uncacheable and certain instruction fetch timing conditions occur, the system may experience unpredictable behavior.

Implication: The type of memory aliasing contributing to this erratum is the case where two different logical processors have the same code page mapped with two different memory types. Specifically, if one code page is mapped by one logical processor as write-back and by another as uncacheable and certain instruction fetch timing conditions occur, the system may experience unpredictable behavior.

Workaround: Code pages should not be mapped with uncacheable and cacheable memory types at the same time.

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

AAJ22. Delivery Status of the LINT0 Register of the Local Vector Table May be Lost

Problem: The Delivery Status bit of the LINT0 Register of the Local Vector Table will not be restored after a transition out of C6 under the following conditions

- LINT0 is programmed as level-triggered
- The delivery mode is set to either Fixed or ExtINT
- There is a pending interrupt which is masked with the interrupt enable flag (IF)

Implication: Due to this erratum, the Delivery Status bit of the LINT0 Register will unexpectedly not be set. Intel has not observed this erratum with any commercially available software or system.

Workaround: None identified.

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

AAJ23. Performance Monitor Event SEGMENT_REG_LOADS Counts Inaccurately

Problem: The performance monitor event SEGMENT_REG_LOADS (Event 06H) counts instructions that load new values into segment registers. The value of the count may be inaccurate.

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

Workaround: None identified.

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

**AAJ24. #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.

AAJ25. Improper Parity Error Signaled in the IQ Following Reset When a Code Breakpoint is Set on a #GP Instruction

Problem: While coming out of cold reset or exiting from C6, if the processor encounters an instruction longer than 15 bytes (which causes a #GP) and a code breakpoint is enabled on that instruction, an IQ (Instruction Queue) parity error may be incorrectly logged resulting in an MCE (Machine Check Exception).

Implication: When this erratum occurs, an MCE may be incorrectly signaled.

Workaround: None identified.

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



AAJ26. An Enabled Debug Breakpoint or Single Step Trap May Be Taken after MOV SS/POP SS Instruction if it is Followed by an Instruction That Signals a Floating Point Exception

Problem: A MOV SS/POP SS instruction should inhibit all interrupts including debug breakpoints until after execution of the following instruction. This is intended to allow the sequential execution of MOV SS/POP SS and MOV [r/e]SP, [r/e]BP instructions without having an invalid stack during interrupt handling. However, an enabled debug breakpoint or single step trap may be taken after MOV SS/POP SS if this instruction is followed by an instruction that signals a floating point exception rather than a MOV [r/e]SP, [r/e]BP instruction. This results in a debug exception being signaled on an unexpected instruction boundary since the MOV SS/POP SS and the following instruction should be executed automatically.

Implication: This can result in incorrect signaling of a debug exception and possibly a mismatched Stack Segment and Stack Pointer. If MOV SS/POP SS is not followed by a MOV [r/e]SP, [r/e]BP, there may be a mismatched Stack Segment and Stack Pointer on any exception. Intel has not observed this erratum with any commercially available software or system.

Workaround: As recommended in the *IA32 Intel® Architecture Software Developer's Manual*, the use of MOV SS/POP SS in conjunction with MOV [r/e]SP, [r/e]BP will avoid the failure since the MOV [r/e]SP, [r/e]BP will not generate a floating point exception. Developers of debug tools should be aware of the potential incorrect debug event signaling created by this erratum.

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

AAJ27. IA32_MPERF Counter Stops Counting During On-Demand TM1

Problem: According to the *Intel® 64 and IA-32 Architectures Software Developer's Manual* Volume 3A: System Programming Guide, the ratio of IA32_MPERF (MSR E7H) to IA32_APERF (MSR E8H) should reflect actual performance while TM1 or on-demand throttling is activated. Due to this erratum, IA32_MPERF MSR stops counting while TM1 or on-demand throttling is activated, and the ratio of the two will indicate higher processor performance than actual.

Implication: The incorrect ratio of IA32_APERF/IA32_MPERF can mislead software P-state (performance state) management algorithms under the conditions described above. It is possible for the Operating System to observe higher processor utilization than actual, which could lead the OS into raising the P-state. During TM1 activation, the OS P-state request is irrelevant and while on-demand throttling is enabled, it is expected that the OS will not be changing the P-state. This erratum should result in no practical implication to software.

Workaround: None identified.

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

**AAJ28. Intel® QuickPath Memory Controller tTHROT_OPREF Timings May be Violated During Self Refresh Entry**

Problem: During self refresh entry, the memory controller may issue more refreshes than permitted by tTHROT_OPREF (bits 29:19 in MC_CHANNEL_{0,1,2}_REFRESH_TIMING CSR).

Implication: The intention of tTHROT_OPREF is to limit current. Since current supply conditions near self refresh entry are not critical, there is no measurable impact due to this erratum.

Workaround: None identified.

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

AAJ29. Processor May Over Count Correctable Cache MESI State Errors

Problem: Under a specific set of conditions, correctable Level 2 cache hierarchy MESI state errors may be counted more than once per occurrence of a correctable error.

Implication: Correctable Level 2 cache hierarchy MESI state errors may be reported in the MCI_STATUS register at a rate higher than their actual occurrence.

Workaround: None identified.

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

AAJ30. Synchronous Reset of IA32_APERF/IA32_MPERF Counters on Overflow Does Not Work

Problem: When either the IA32_MPERF or IA32_APERF MSR (E7H, E8H) increments to its maximum value of 0xFFFF_FFFF_FFFF_FFFF, both MSRs are supposed to synchronously reset to 0x0 on the next clock. This synchronous reset does not work. Instead, both MSRs increment and overflow independently.

Implication: Software can not rely on synchronous reset of the IA32_APERF/IA32_MPERF registers.

Workaround: None identified.

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

**AAJ31. Disabling Thermal Monitor While Processor is Hot, Then Re-enabling, May Result in Stuck Core Operating Ratio**

Problem: If a processor is at its TCC (Thermal Control Circuit) activation temperature and then Thermal Monitor is disabled by a write to IA32_MISC_ENABLE MSR (1A0H) bit [3], a subsequent re-enable of Thermal Monitor will result in an artificial ceiling on the maximum core P-state. The ceiling is based on the core frequency at the time of Thermal Monitor disable. This condition will only correct itself once the processor reaches its TCC activation temperature again.

Implication: Since Intel requires that Thermal Monitor be enabled in order to be operating within specification, this erratum should never be seen during normal operation.

Workaround: Software should not disable Thermal Monitor during processor operation.

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

AAJ32. The PECI Throttling Counter May Not be Accurate

Problem: Under certain throttling circumstances, the PECI (Platform Environment Control Interface) throttling counter may not be accurate. If the throttling counter is zero, then the counter accurately reflects that throttling never occurred.

Implication: If the PECI throttle counter is non-zero, it 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.

AAJ33. PECI Does Not Support PCI Configuration Reads/Writes to Misaligned Addresses

Problem: The PECI (Platform Environment Control Interface) specification allows for partial reads from or writes to misaligned addresses within the PCI configuration space. However, the PECI client does not properly interpret addresses that are Dword (4 byte) misaligned and may read or write incorrect data.

Implication: Due to this erratum, writes to or reads from Dword misaligned addresses could result in unintended side effects and unpredictable behavior.

Workaround: PECI host controllers may issue byte, word and Dword reads and writes as long as they are aligned to Dword addresses.

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

**AAJ34. OVER Bit for IA32_MCi_STATUS Register May Get Set on Specific Internal Error**

Problem: If a specific type of internal unclassified error is detected, as identified by IA32_MCi_STATUS.MCACOD=0x0405, the IA32_MCi_STATUS.OVER (overflow) bit [62] may be erroneously set.

Implication: The OVER bit of the MCI_STATUS register may be incorrectly set for a specific internal unclassified error.

Workaround: None identified.

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

AAJ35. Writing the Local Vector Table (LVT) when an Interrupt is Pending May Cause an Unexpected Interrupt

Problem: If a local interrupt is pending when the LVT entry is written, an interrupt may be taken on the new interrupt vector even if the mask bit is set.

Implication: An interrupt may immediately be generated with the new vector when a LVT entry is written, even if the new LVT entry has the mask bit set. If there is no Interrupt Service Routine (ISR) set up for that vector the system will GP fault. If the ISR does not do an End of Interrupt (EOI) the bit for the vector will be left set in the in-service register and mask all interrupts at the same or lower priority.

Workaround: Any vector programmed into an LVT entry must have an ISR associated with it, even if that vector was programmed as masked. This ISR routine must do an EOI to clear any unexpected interrupts that may occur. The ISR associated with the spurious vector does not generate an EOI, therefore the spurious vector should not be used when writing the LVT.

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

AAJ36. A Processor Core May Not Wake Up from S1 State

Problem: If there is an interrupt pended at the same time as the package is entering S1 and one of the cores in the package is entering C3, it is possible that the core entering C3 may not wake up from the S1 state.

Implication: Due to this erratum, the processor core may not wake up from S1 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.

**AAJ37. Reading Reserved APIC Registers May Not Signal an APIC Error**

Problem: Reads of reserved APIC registers in xAPIC compatibility mode should signal an APIC error with the Illegal Register Address bit [11] set in the Error Status Register (offset 0x280). Due to the erratum, the error is neither logged nor signaled.

Implication: A reserved APIC register access error interrupt may not be logged or signaled, even though the APIC error interrupt is enabled, on a read of a reserved APIC register.

Workaround: None identified.

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

AAJ38. A Logical Processor Receiving a SIPI After a VM Entry Into WFS State May Become Unresponsive

Problem: A logical processor may become unresponsive after receiving a SIPI (Start-up Interprocessor Interrupt) following a VM Entry into a WFS (Wait-for-SIPI) state.

Implication: The logical processor that receives a SIPI while in the WFS state may stop responding.

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.

AAJ39. Memory Controller May Deliver Incorrect Data When Memory Ranks Are In Power-Down

Problem: When one or more memory ranks are in Power-Down (as controlled by MC_CHANNEL_{0,1,2}_CKE_TIMING CSR parameters), certain memory access patterns may result in incorrect data.

Implication: Due this erratum, incorrect data may result.

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.

**AAJ40. Faulting MMX Instruction May Incorrectly Update x87 FPU Tag Word**

Problem: Under a specific set of conditions, MMX stores (MOVD, MOVQ, MOVNTQ, MASKMOVQ) which cause memory access faults (#GP, #SS, #PF, or #AC), may incorrectly update the x87 FPU tag word register.

This erratum will occur when the following additional conditions are also met.

- The MMX store instruction must be the first MMX instruction to operate on x87 FPU state (i.e. the x87 FP tag word is not already set to 0x0000).
- For MOVD, MOVQ, MOVNTQ stores, the instruction must use an addressing mode that uses an index register (this condition does not apply to MASKMOVQ).

Implication: If the erratum conditions are met, the x87 FPU tag word register may be incorrectly set to a 0x0000 value when it should not have been modified.

Workaround: None identified.

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

AAJ41. A Floating-Point Store Instruction May Cause an Unexpected x87 FPU Floating-Point Error (#MF)

Problem: If a floating-point store instruction (FST or FSTP) causes an inexact-result exception (#P) and such exceptions are unmasked, the next "waiting" x87 FPU instruction or WAIT/FWAIT instruction will incur an x87 FPU Floating-Point Error (#MF). Due to this erratum, the #MF may occur prematurely and prevent the floating-point store instruction from executing. This may occur when the logical processor is in VMX non-root operation and either (1) the "use EPT" VM-execution control is 1; or (2) the "virtual APIC accesses" VM-execution control is 1 and the store is to the APIC-access page.

Implication: Due to this erratum, a floating-point store instruction may cause a #MF that should be held pending until the next "waiting" x87 FPU instruction or WAIT/FWAIT instruction.

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.

AAJ42. Incorrect TLB Translation May Occur After Exit From C6

Problem: Under certain conditions when C6 and two logical processors on the same core are enabled on a processor, an instruction fetch occurring after a logical processor exits from C6 may incorrectly use the translation lookaside buffer (TLB) address mapping belonging to the other logical processor in the processor core.

Implication: When this erratum occurs, unpredictable behavior may result.

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.

**AAJ43. USB 1.1 ISOCH Audio Glitches with Intel® QuickPath Interconnect Locks and Deep C-States**

Problem: An interrupt directed at a Core in C3 or C6 that collides with an Intel® QuickPath Interconnect Lock sequence may delay ISOCH transactions to DRAM long enough to underrun USB 1.1 buffers.

Implication: USB 1.1 Audio devices may have audio glitches.

Workaround: None identified.

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

AAJ44. Stack Pointer May Become Incorrect In Loops With Unbalanced Push and Pop Operations

Problem: If a loop has an unbalanced number of Push and Pop operations, under a specific set of conditions, it is possible that the stack pointer (SP/ESP/RSP) may become incorrect.

Implication: When this erratum occurs, unpredictable behavior may result. 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.

AAJ45. A P-state Change While Another Core is in C6 May Prevent Further C-state and P-state Transitions

Problem: Under a specific set of conditions, when one core is in C6 and another core transitions from P_n to a non-P_n ratio, further C-state and P-state changes may be blocked.

Implication: The processor may stop responding to additional requests for deeper sleep 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.

AAJ46. Certain Store Parity Errors May Not Log Correct Address in IA32_MCi_ADDR

Problem: When store parity errors in the Level 0 hierarchy (as defined in the LL subfield of the IA32_MCi_STATUS MSR) occur, it is possible that the address of the error will not be logged in IA32_MCi_ADDR MSR. The error itself will be logged properly.

Implication: The address in IA32_MCi_ADDR may be incorrect after certain store parity errors occur.

Workaround: None identified.

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

**AAJ47. xAPIC Timer May Decrement Too Quickly Following an Automatic Reload While in Periodic Mode**

Problem: When the xAPIC Timer is automatically reloaded by counting down to zero in periodic mode, the xAPIC Timer may slip in its synchronization with the external clock. The xAPIC timer may be shortened by up to one xAPIC timer tick.

Implication: When the xAPIC Timer is automatically reloaded by counting down to zero in periodic mode, the xAPIC Timer may slip in its synchronization with the external clock. The xAPIC timer may be shortened by up to one xAPIC timer tick.

Workaround: None identified.

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

AAJ48. Certain Undefined Opcodes Crossing a Segment Limit May Result in #UD Instead of #GP Exception

Problem: Processor may take a #UD (Invalid Opcode) exception instead of a #GP (General Protection) exception when certain undefined opcodes (opcodes 0F 01 D0 - 0F 01 D5) extend beyond the segment limit.

Implication: Due to this erratum, processor may not take a #GP exception in this situation.

Workaround: None identified.

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

AAJ49. Indication of A20M Support is Inverted

Problem: The value read back from VLW_CAPABILITY MSR (1F0H) bit [1] (A20M support) is inverted. Therefore, reading back a '1' (which should indicate A20M is supported) actually indicates A20M is not supported, and vice versa.

Implication: Software relying on this bit to determine whether A20M feature is supported by the processor will read back the opposite value of what is supported.

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.

**AAJ50. Reported Memory Type May Not Be Used to Access the VMCS and Referenced Data Structures**

Problem: Bits 53:50 of the IA32_VMX_BASIC MSR report the memory type that the processor uses to access the VMCS and data structures referenced by pointers in the VMCS. Due to this erratum, a VMX access to the VMCS or referenced data structures will instead use the memory type that the MTRRs (memory-type range registers) specify for the physical address of the access.

Implication: Bits 53:50 of the IA32_VMX_BASIC MSR report that the WB (write-back) memory type will be used but the processor may use a different memory type.

Workaround: Software should ensure that the VMCS and referenced data structures are located at physical addresses that are mapped to WB memory type by the MTRRs.

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

AAJ51. After VM Entry, Instructions May Incorrectly Operate as if CS.D=0

Problem: If bit 13 (L) and bit 14 (D/B) of the guest CS access rights field in the VMCS are both 1 and VM entry takes the processor out of IA-32e mode, instructions executed after VM entry may operate as if CS.D=0.

Implication: Instructions executed after VM entry may use the wrong operation size. 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.

AAJ52. Spurious Machine Check Error May Occur When Logical Processor is Woken Up

Problem: The first time a logical processor is woken up after power on (including resume from system sleep states) an Internal Parity Error may be detected and logged when no real parity error occurred.

Implication: When this erratum occurs, a spurious Internal Parity Error may be logged. However, no machine check exception will be signaled in this case.

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.

**AAJ53. B0-B3 Bits in DR6 For Non-Enabled Breakpoints May be Incorrectly Set**

Problem: Some of the B0-B3 bits (breakpoint conditions detect flags, bits [3:0]) in DR6 may be incorrectly set for non-enabled breakpoints when the following sequence happens:

1. MOV or POP instruction to SS (Stack Segment) selector;
2. Next instruction is FP (Floating Point) that gets FP assist
3. Another instruction after the FP instruction completes successfully
4. A breakpoint occurs due to either a data breakpoint on the preceding instruction or a code breakpoint on the next instruction.

Due to this erratum a non-enabled breakpoint triggered on step 1 or step 2 may be reported in B0-B3 after the breakpoint occurs in step 4.

Implication: Due to this erratum, B0-B3 bits in DR6 may be incorrectly set for non-enabled breakpoints.

Workaround: Software should not execute a floating point instruction directly after a MOV SS or POP SS instruction.

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

AAJ54. Core C6 May Clear Previously Logged TLB Errors

Problem: Following an exit from core C6, previously logged TLB (Translation Lookaside Buffer) errors in IA32_MCi_STATUS may be cleared.

Implication: Due to this erratum, TLB errors logged in the associated machine check bank prior to core C6 entry may be cleared. Provided machine check exceptions are enabled, the machine check exception handler can log any uncorrectable TLB errors prior to core C6 entry. The TLB marks all detected errors as uncorrectable.

Workaround: As long as machine check exceptions are enabled, the machine check exception handler can log the TLB error prior to core C6 entry. This will ensure the error is logged before it is cleared.

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

AAJ55. Processor May Hang When Two Logical Processors Are in Specific Low Power States

Problem: When two logical processors in a physical core have entered the C1 and C6 idle states respectively, it is possible that the processor may hang and log a machine check error with IA32_MCi_STATUS.MCACOD = 0x0106. The error does not occur when either core has entered C3 or when both logical processors enter the same idle state.

Implication: Due to this erratum, a hang may occur and a machine check may be logged while two logical processors are in a low power 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.

**AAJ56. MOVNTDQA From WC Memory May Pass Earlier Locked Instructions**

Problem: An execution of MOVNTDQA that loads from WC (write combining) memory may appear to pass an earlier locked instruction to a different cache line.

Implication: Software that expects a lock to fence subsequent MOVNTDQA instructions may not operate properly. If the software does not rely on locked instructions to fence the subsequent execution of MOVNTDQA then this erratum does not apply.

Workaround: Software that requires a locked instruction to fence subsequent executions of MOVNTDQA should insert an LFENCE instruction before the first execution of MOVNTDQA following the locked instruction. If there is already a fencing or serializing instruction between the locked instruction and the MOVNTDQA, then an additional LFENCE is not necessary.

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

AAJ57. Performance Monitor Event MISALIGN_MEM_REF May Over Count

Problem: The MISALIGN_MEM_REF Performance Monitoring (Event 05H) may over count memory misalignment events, possibly by orders of magnitude.

Implication: Software relying on MISALIGN_MEM_REF to count cache line splits for optimization purposes may read excessive number of memory misalignment events.

Workaround: None identified.

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

AAJ58. 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.

**AAJ59. Writes to IA32_CR_PAT or IA32_EFER MSR May Cause an Incorrect ITLB Translation**

Problem: Under certain conditions, writes to IA32_CR_PAT (277H) or IA32_EFER (C000080H) MSRs may result in an incorrect ITLB (instruction translation lookaside buffer) translation.

Implication: Due this erratum, unpredictable system behavior may occur.

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

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

AAJ60. The "Virtualize APIC Accesses" VM-Execution Control May be Ignored

Problem: If a VM exit occurs while the "virtualize APIC accesses" and "enable VPID" VM-execution controls are both 1 and the VM-exit MSR-store count is not 0, the logical processor may operate as if the "virtualize APIC accesses" VM-execution control was 0 following a subsequent VM entry.

Implication: This erratum may prevent VMM software from virtualizing memory-mapped APIC accesses if it is using VPIDs (virtual-processor identifiers) and is saving MSRs on VM exits.

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.

AAJ61. C6 Transitions May Cause Spurious Updates to the xAPIC Error Status Register

Problem: If any of the LVT entries are not initialized, reads from xAPIC Error Status Register following a C6 transition may report a spurious illegal vector received.

Implication: Due to this erratum, reads to xAPIC Error Status Register may report illegal vector received when none was actually received.

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.

AAJ62. Critical ISOCH Traffic May Cause Unpredictable System Behavior When Write Major Mode Enabled

Problem: Under a specific set of conditions, critical ISOCH (isochronous) traffic may cause unpredictable system behavior with write major mode enabled.

Implication: Due to this erratum unpredictable system behavior may occur.

Workaround: Write major mode must be disabled in the BIOS by writing the write major mode threshold value to its maximum value of 1FH in ISOCHEXITTHRESHOLD bits [19:15], ISOCHENTRYTHRESHOLD bits [14:10], WMENTRYTHRESHOLD bits [9:5], and WMEXITTHRESHOLD bits [4:0] of the MC_CHANNEL_{0,1,2}_WAQ_PARAMS register.

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

**AAJ63. Running with Write Major Mode Disabled May Lead to a System Hang**

Problem: With write major mode disabled, reads will be favored over writes and under certain circumstances this can lead to a system hang.

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.

AAJ64. Memory Controller Address Parity Error Injection Does Not Work Correctly

Problem: When MC_CHANNEL_{0,1,2}_ECC_ERROR_INJECT.INJECT_ADDR_PARITY bit [4] = 1 an error may be injected on any command on the channel and not just RD or WR CAS commands that match MC_CHANNEL_{0,1,2}_ADDR_MATCH.

Implication: Address parity error injection cannot be used to reliably target a DIMM or memory location within a channel. When the address parity errors occur, the IA32_MCi_MISC register reflects the DIMM ID of the DIMM that detected error and not necessarily the DIMM that was targeted by the error injection settings.

Workaround: None identified.

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

AAJ65. Memory Controller Opportunistic Refreshes Might be Missed

Problem: If a system meets all 3 conditions below, opportunistic refresh capability might be degraded.

1. 2x refresh enabled and opportunistic refreshes enabled through tTHROT_OPPREFRESH field in the MC_CHANNEL_{0,1,2}_REFRESH_TIMING
2. DDR3-800 DIMMS or DDR3-1066 DIMMS with tREFI value programmed more than 5% lower than the nominal value
3. More than 2 DIMMs populated

Implication: Due to this erratum, a corner condition can cause a persistent degradation of opportunistic refresh capability.

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.

**AAJ66. Delivery of Certain Events Immediately Following a VM Exit May Push a Corrupted RIP Onto The Stack**

Problem: If any of the following events is delivered immediately following a VM exit to 64-bit mode from outside 64-bit mode, bits 63:32 of the RIP value pushed on the stack may be cleared to 0:

4. A non-maskable interrupt (NMI);
5. A machine-check exception (#MC);
6. A page fault (#PF) during instruction fetch; or
7. A general-protection exception (#GP) due to an attempt to decode an instruction whose length is greater than 15 bytes.

Implication: Unexpected behavior may occur due to the incorrect value of the RIP on the stack. Specifically, return from the event handler via IRET may encounter an unexpected page fault or may begin fetching from an unexpected code address.

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.

AAJ67. The Combination of a Bus Lock and a Data Access That is Split Across Page Boundaries May Lead to Processor Livelock

Problem: Under certain complex micro-architectural conditions, the coincidence of a bus lock initiated by one logical processor of a Hyper-threading enabled processor core and data accesses that are split across page boundaries, initiated on the other logical processor on the same core, may lead to processor livelock.

Implication: Due to this erratum, a livelock may occur that can only be terminated by a processor reset. 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.

AAJ68. CPUID Instruction Returns Incorrect Brand String

Problem: When a CPUID instruction is executed with EAX = 80000002H, 80000003H and 80000004H, the return values contain the brand string Intel(R) Core(TM) CPU when it should have Intel(R) Core(TM) i7 CPU. In addition, the processor number will be incorrect. The return value will have an additional zero between the processor number and the @ symbol (for example: Intel(R) Core(TM) CPU nnn0 @ x.xx GHz where nnn is a processor number and x.xx is the frequency).

Implication: When this erratum occurs, the processor will report the incorrect brand string.

Workaround: None identified.

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

**AAJ69. An Unexpected Page Fault May Occur Following the Unmapping and Re-mapping of a Page**

- Problem:** An unexpected page fault (#PF) may occur for a page under the following conditions:
- The paging structures initially specify a valid translation for the page.
 - Software modifies the paging structures so that there is no valid translation for the page (e.g., by clearing to 0 the present bit in one of the paging-structure entries used to translate the page).
 - Software later modifies the paging structures so that the translation is again a valid translation for the page (e.g., by setting to 1 the bit that was cleared earlier).
 - A subsequent instruction loads from a linear address on the page.
 - Software did not invalidate TLB entries for the page between the first modification of the paging structures and the load from the linear address.

In this case, the load by the later instruction may cause a page fault that indicates that there is no translation for the page.

Implication: Software may see an unexpected page fault that indicates that there is no translation for the page.

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.

AAJ70. Infinite Stream of Interrupts May Occur if an ExtINT Delivery Mode Interrupt is Received while All Cores in C6

Problem: If all logical processors in a core are in C6, an ExtINT delivery mode interrupt is pending in the xAPIC and interrupts are blocked with EFLAGS.IF=0, the interrupt will be processed after C6 wakeup and after interrupts are re-enabled (EFLAGS.IF=1). However, the pending interrupt event will not be cleared.

Implication: Due to this erratum, an infinite stream of interrupts will occur on the core servicing the external interrupt. Intel has not observed this erratum with any commercially available software/system.

Workaround: None identified.

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

**AAJ71. Two xAPIC Timer Event Interrupts May Unexpectedly Occur**

Problem: If an xAPIC timer event is enabled and while counting down the current count reaches 1 at the same time that the processor thread begins a transition to a low power C-state, the xAPIC may generate two interrupts instead of the expected one when the processor returns to C0.

Implication: Due to this erratum, two interrupts may unexpectedly be generated by an xAPIC timer event.

Workaround: None identified.

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

AAJ72. EOI Transaction May Not be Sent if Software Enters Core C6 During an Interrupt Service Routine

Problem: If core C6 is entered after the start of an interrupt service routine but before a write to the APIC EOI (End of Interrupt) register, and the core is woken up by an event other than a fixed interrupt source the core may drop the EOI transaction the next time APIC EOI register is written and further interrupts from the same or lower priority level will be blocked.

Implication: EOI transactions may be lost and interrupts may be blocked when core C6 is used during interrupt service routines.

Workaround: Software should check the ISR register and if any interrupts are in service only enter C1.

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

AAJ73. 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.

**AAJ74. PEBS Records For Load Latency Monitoring May Contain an Incorrect Linear Address**

Problem: The load latency performance monitoring feature stores information about a load into a record in the PEBS (Precise event-based sampling) buffer in the DS save area. This information includes the Data Source Encoding, Latency Value, and Data Linear Address of the load causing the performance counter to overflow. Under certain conditions it is possible for the linear address to be incorrect.

Implication: The linear address reported by the load latency performance monitoring feature for PEBS 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.

AAJ75. PEBS Field "Data Linear Address" is Not Sign Extended to 64 Bits

Problem: The Data Linear Address field of the PEBS (Precise Event-Based Sampling) record is not correctly sign extended to 64 bits and may appear as a non-canonical address when observed in the PEBS record.

Implication: The PEBS Data Linear Address field may not have the sign bit correctly extended to bits [63:48].

Workaround: None identified.

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

AAJ76. Core C6 May Not Operate Correctly in the Presence of Bus Locks

Problem: The processor state may be incorrect after core C6 exit if system bus locks are in progress at the time of core C6 entry.

Implication: The processor may begin fetching from the wrong address or have incorrect state after an exit from core C6.

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.

AAJ77. Intel® Turbo Boost Technology May be Limited Immediately After Package C-state Exit with QPI L1 Mode Disabled

Problem: If the processor is resident in package C3 or C6 for greater than 100ms and Intel® QPI (Intel® QuickPath Interconnect) link L1 mode is disabled, it is possible for Turbo Boost input parameters to be incorrect. As a result, on exit from the package C-state the processor may not enter Turbo Boost for up to 2 ms.

Implication: Turbo Boost may be limited after exiting a package C-state (C3 and C6) that lasted longer than 100 ms.

Workaround: None identified.

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

**AAJ78. 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.

AAJ79. CPUID Incorrectly Indicates the UnHalted Reference Cycle Architectural Event is Supported

Problem: The architectural performance monitoring event for UnHalted Reference Cycles (3CH, Umask 01H) is not supported on the processor. The CPUID instruction, when executed with EAX = 0AH, should return bit 2 of EBX as 1 to indicate that this event is not supported. Due to this erratum, CPUID will improperly return bit 2 as 0.

Implication: Software relying on the CPUID instruction to determine support of the UnHalted Reference Cycles event will incorrectly assume the event is available.

Workaround: None identified.

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

AAJ80. Architectural Performance Monitor Event ‘Branch Misses Retired’ is Counted Incorrectly

Problem: The Architectural Performance Monitor Event ‘branch misses retired’ (Event C5H) is not counted correctly and may result in an under count or an over count.

Implication: The Architectural Performance Monitor Event ‘branch misses retired’ will not show accurate results when counted.

Workaround: It is possible for the BIOS to contain a workaround for this erratum which reports via CPUID that this event is not available.

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

**AAJ81. DR6.B0-B3 May Not Report All Breakpoints Matched When a MOV/POP SS is Followed by a Store Instruction**

Problem: Normally, data breakpoints matches 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 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.

AAJ82. 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.

AAJ83. IA32_PERF_GLOBAL_CTRL MSR May be Incorrectly Initialized

Problem: The IA32_PERF_GLOBAL_CTRL MSR (38FH) bits [34:32] may be incorrectly set to 7H after reset; the correct value should be 0H.

Implication: The IA32_PERF_GLOBAL_CTRL MSR bits [34:32] may be incorrect after reset (EN_FIXED_CTR{0, 1, 2} may be enabled).

Workaround: None identified.

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

**AAJ84. Performance Monitor Interrupts Generated From Uncore Fixed Counters (394H) May be Ignored**

Problem: Performance monitor interrupts (PMI's) from Uncore fixed counters are ignored when Uncore general performance monitor counters 3B0H-3BFH are not programmed.

Implication: This erratum blocks a usage model in which each of the cores can sample its own performance monitor events synchronously based on single interrupt from the Uncore.

Workaround: Program any one of the Uncore general performance monitor counters with a valid performance monitor event and enable the event by setting the local enable bit in the corresponding performance monitor event select MSR. For the usage model where no counting is desired, program that Uncore general performance counter's global enable bit to be zero.

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

AAJ85. Processors with SMT May Hang on P-State Transition or ACPI Clock Modulation Throttling

Problem: When SMT is enabled, it is possible that a P-state transition or ACPI clock modulation throttling may hang and log a machine check error with IA32_MCi_STATUS.MCACOD = 0x0150. This hang condition requires a specific sequence of instructions coincident with the P-state or ACPI event.

Implication: When this erratum occurs, the processor will unexpectedly hang. 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.

AAJ86. Performance Monitor Counter INST_RETIRED.STORES May Count Higher than Expected

Problem: Performance Monitoring counter INST_RETIRED.STORES (Event: C0H) is used to track retired instructions which contain a store operation. Due to this erratum, the processor may also count other types of instructions including WRMSR and MFENCE.

Implication: Performance Monitoring counter INST_RETIRED.STORES may report counts higher than expected.

Workaround: None identified.

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

**AAJ87. Sleeping Cores May Not be Woken Up on Logical Cluster Mode Broadcast IPI Using Destination Field Instead of Shorthand**

Problem: If software sends a logical cluster broadcast IPI using a destination shorthand of 00B (No Shorthand) and writes the cluster portion of the Destination Field of the Interrupt Command Register to all ones while not using all 1s in the mask portion of the Destination Field, target cores in a sleep state that are identified by the mask portion of the Destination Field may not be woken up. This erratum does not occur if the destination shorthand is set to 10B (All Including Self) or 11B (All Excluding Self).

Implication: When this erratum occurs, cores which are in a sleep state may not wake up to handle the broadcast IPI. Intel has not observed this erratum with any commercially available software.

Workaround: Use destination shorthand of 10B or 11B to send broadcast IPIs.

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

AAJ88. Faulting Executions of FXRSTOR May Update State Inconsistently

Problem: The state updated by a faulting FXRSTOR instruction may vary from one execution to another.

Implication: Software that relies on x87 state or SSE state following a faulting execution of FXRSTOR may behave inconsistently.

Workaround: Software handling a fault on an execution of FXRSTOR can compensate for execution variability by correcting the cause of the fault and executing FXRSTOR again.

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

AAJ89. Unexpected QPI Link Behavior May Occur When a CRC Error Happens During L0s

Problem: When a QPI (Intel® QuickPath Interconnect) agent requests L0s entry while a CRC (Cyclic Redundancy Check) error occurs during this flit or on the flit just before it, the requesting QPI agent may enter L0s and turn its drivers off. During this time noise on the link may be interpreted as a QPI command by the remote QPI agent, and may result in unexpected behavior.

Implication: Unexpected QPI link behavior may occur when CRC error happens on or just before L0s entry request.

Workaround: Disable L0s.

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

**AAJ90. Performance Monitor Event EPT.EPDPE_MISS May be Counted While EPT is Disabled**

Problem: Performance monitor event EPT.EPDPE_MISS (Event: 4FH, Umask: 08H) is used to count Page Directory Pointer table misses while EPT (extended page tables) is enabled. Due to this erratum, the processor will count Page Directory Pointer table misses regardless of whether EPT is enabled or not.

Implication: Due to this erratum, performance monitor event EPT.EPDPE_MISS may report counts higher than expected.

Workaround: Software should ensure this event is only enabled while in EPT mode.

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

AAJ91. Performance Monitor Counters May Count Incorrectly

Problem: Under certain circumstances, a general purpose performance counter, IA32_PMC0-4 (C1H – C4H), may count at core frequency or not count at all instead of counting the programmed event.

Implication: The Performance Monitor Counter IA32_PMCx may not properly count the programmed event. Due to the requirements of the workaround there may be an interruption in the counting of a previously programmed event during the programming of a new event.

Workaround: Before programming the performance event select registers, IA32_PERFEVTSELx MSR (186H – 189H), the internal monitoring hardware must be cleared. This is accomplished by first disabling, saving valid events and clearing from the select registers, then programming three event values 0x4300D2, 0x4300B1 and 0x4300B5 into the IA32_PERFEVTSELx MSRs, and finally continuing with new event programming and restoring previous programming if necessary. Each performance counter, IA32_PMCx, must have its corresponding IA32_PREFEVTSELx MSR programmed with at least one of the event values and must be enabled in IA32_PERF_GLOBAL_CTRL MSR (38FH) bits [3:0]. All three values must be written to either the same or different IA32_PERFEVTSELx MSRs before programming the performance counters. Note that the performance counter will not increment when its IA32_PERFEVTSELx MSR has a value of 0x4300D2, 0x4300B1 or 0x4300B5 because those values have a zero UMASK field (bits [15:8]).

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

**AAJ92. Processor Forward Progress Mechanism Interacting With Certain MSR/CSR Writes May Cause Unpredictable System Behavior**

Problem: Under specific internal conditions, a mechanism within the processor to ensure forward progress may interact with writes to a limited set of MSRs/CSRs and consequently may lead to unpredictable system behavior.

Implication: This erratum may cause 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.

AAJ93. USB 1.1 Isoch Memory Latencies May Increase During Package C3/C6 Transitions

Problem: USB 1.1 Isoch memory response latencies may increase during package C3/C6 transitions due to non-optimal C3/C6 Exit operation.

Implication: Increased Isoch latencies may cause perturbations in system operation. (ex: audio glitches.)

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.

AAJ94. Processor May Incorrectly Demote Processor C6 State to a C3 State

Problem: The auto demotion feature on the processor demotes processor C6 C-state requests to C3 in a more aggressive manner than expected, leading to low C6 residency.

Implication: Due to this erratum, the system may exhibit higher than expected idle power due to low C6 residency.

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

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

AAJ95. Performance Monitor Event Offcore_response_0 (B7H) Does Not Count NT Stores to Local DRAM Correctly

Problem: When a IA32_PERFEVTSELx MSR is programmed to count the Offcore_response_0 event (Event:B7H), selections in the OFFCORE_RSP_0 MSR (1A6H) determine what is counted. The following two selections do not provide accurate counts when counting NT (Non-Temporal) Stores:

- OFFCORE_RSP_0 MSR bit [14] is set to 1 (LOCAL_DRAM) and bit [7] is set to 1 (OTHER): NT Stores to Local DRAM are not counted when they should have been.
- OFFCORE_RSP_0 MSR bit [9] is set to (OTHER_CORE_HIT_SNOOP) and bit [7] is set to 1 (OTHER): NT Stores to Local DRAM are counted when they should not have been.

Implication: The counter for the Offcore_response_0 event may be incorrect for NT stores.

Workaround: None identified.

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

**AAJ96. 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.

AAJ97. System May Hang if MC_CHANNEL_{0,1,2}_MC_DIMM_INIT_CMD.DO_ZQCL Commands Are Not Issued in Increasing Populated DDR3 Rank Order

Problem: ZQCL commands are used during initialization to calibrate DDR3 termination. A ZQCL command can be issued by writing 1 to the MC_CHANNEL_{0,1,2}_MC_DIMM_INIT_CMD.DO_ZQCL (Device 4,5,6, Function 0, Offset 15, bit[15]) field and it targets the DDR3 rank specified in the RANK field (bits[7:5]) of the same register. If the ZQCL commands are not issued in increasing populated rank order then ZQ calibration may not complete, causing the system to hang.

Implication: Due to this erratum the system may hang if writes to the MC_CHANNEL_{0,1,2}_MC_DIMM_INIT_CMD.DO_ZQCL field are not in increasing populated DDR3 rank order.

Workaround: It is possible for Intel provided BIOS reference code to contain a workaround for this erratum. Please refer to the latest version of BIOS Memory Reference Code and release notes.

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

**AAJ98. LER and LBR MSRs May Be Incorrectly Updated During a Task Switch**

Problem: LER (Last Exception Record) and LBR (Last Branch Record) MSRs (MSR_LER_FROM_LIP (1DDH), MSR_LER_TO_LIP (1DEH) and MSR_LASTBRANCH{0:15}_FROM_IP (680H – 68FH)) may contain incorrect values after a fault or trap that does a task switch.

Implication: After a task switch the value of the LER and LBR MSRs may be updated to point to incorrect instructions.

Workaround: None identified.

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

AAJ99. Virtualized WRMSR to the IA32_EXT_XAPIC_TPR MSR Uses Incorrect Value for TPR Threshold

Problem: If the “virtualize x2APIC mode” VM-execution control is 1, an attempt to write to the IA32_EXT_XAPIC_TPR MSR (808H) using the WRMSR instruction should cause a trap-like VM exit if it reduces the value of the TPR shadow below that of the TPR threshold VM-execution control field. Due to this erratum, such a VM exit may fail to occur when specified. In addition, such a VM exit may occur even if the TPR shadow is not reduced below the TPR threshold.

Implication: Failure to cause the specified VM exits may prevent a virtual-machine monitor (VMM) from delivering virtual interrupts in a timely manner. Generation of incorrect VM exits may cause a VMM to deliver virtual interrupts to a guest prematurely.

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.

AAJ100. Back to Back Uncorrected Machine Check Errors May Overwrite IA32_MC3_STATUS.MSCOD

Problem: When back-to-back uncorrected machine check errors occur that would both be logged in the IA32_MC3_STATUS MSR (40CH), the IA32_MC3_STATUS.MSCOD (bits [31:16]) field may reflect the status of the most recent error and not the first error. The rest of the IA32_MC3_STATUS MSR contains the information from the first error.

Implication: Software should not rely on the value of IA32_MC3_STATUS.MSCOD if IA32_MC3_STATUS.OVER (bit [62]) is set.

Workaround: None identified.

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

**AAJ101. Memory Intensive Workloads with Core C6 Transitions May Cause System Hang**

Problem: Under a complex set of internal conditions, a system running a high cache stress and I/O workload combined with the presence of frequent core C6 transitions may result in a system hang.

Implication: Due to this erratum, the system 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.

AAJ102. Corrected Errors With a Yellow Error Indication May be Overwritten by Other Corrected Errors

Problem: A corrected cache hierarchy data or tag error that is reported with IA32_MCi_STATUS.MCACOD (bits [15:0]) with value of 000x_0001_xxxx_xx01 (where x stands for zero or one) and a yellow threshold-based error status indication (bits [54:53] equal to 10B) may be overwritten by a corrected error with a no tracking indication (00B) or green indication (01B).

Implication: Corrected errors with a yellow threshold-based error status indication may be overwritten by a corrected error without a yellow indication.

Workaround: None identified.

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

AAJ103. PSI# Signal May Incorrectly be Left Asserted

Problem: When some of the cores in the processor are in C3/C6 state, the PSI# (Power Status Indicator) signal may incorrectly be left asserted when another core makes a frequency change request without changing the operating voltage. Since this erratum results in a possible maximum core current greater than the PSI# threshold of 20A, PSI# should have been de-asserted.

Implication: Due to this erratum, platform voltage regulator tolerances may be exceeded and a subsequent system reset 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.



AAJ104. A String Instruction that Re-maps a Page May Encounter an Unexpected Page Fault

- Problem:** An unexpected page fault (#PF) may occur for a page under the following conditions:
- The paging structures initially specify a valid translation for the page.
 - Software modifies the paging structures so that there is no valid translation for the page (e.g., by clearing to 0 the present bit in one of the paging-structure entries used to translate the page).
 - An iteration of a string instruction modifies the paging structures so that the translation is again a valid translation for the page (e.g., by setting to 1 the bit that was cleared earlier).
 - A later iteration of the same string instruction loads from a linear address on the page.
 - Software did not invalidate TLB entries for the page between the first modification of the paging structures and the string instruction. In this case, the load in the later iteration may cause a page fault that indicates that there is no translation for the page (e.g., with bit 0 clear in the page-fault error code, indicating that the fault was caused by a not-present page).

Implication: Software may see an unexpected page fault that indicates that there is no translation for the page. Intel has not observed this erratum with any commercially available software or system.

Workaround: Software should not update the paging structures with a string instruction that accesses pages mapped the modified paging structures.

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

AAJ105. Performance Monitor Events DCACHE_CACHE_LD and DCACHE_CACHE_ST May Overcount

Problem: The performance monitor events DCACHE_CACHE_LD (Event 40H) and DCACHE_CACHE_ST (Event 41h) count cacheable loads and stores that hit the L1 cache. Due to this erratum, in addition to counting the completed loads and stores, the counter will incorrectly count speculative loads and stores that were aborted prior to completion.

Implication: The performance monitor events DCACHE_CACHE_LD and DCACHE_CACHE_ST may reflect a count higher than the actual number of events.

Workaround: None identified.

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

**AAJ106. Rapid Core C3/C6 Transition May Cause Unpredictable System Behavior**

Problem: Under a complex set of internal conditions, cores rapidly performing C3/C6 transitions in a system with Intel® Hyper-Threading Technology enabled may cause a machine check error (IA32_MCi_STATUS.MCACOD = 0x0106), system hang or unpredictable system behavior.

Implication: This erratum may cause a machine check error, system hang or 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 Tables of Changes.

AAJ107. Performance Monitor Events INSTR_RETIRED and MEM_INST_RETIRED May Count Inaccurately

Problem: The performance monitor event INSTR_RETIRED (Event C0H) should count the number of instructions retired, and MEM_INST_RETIRED (Event 0BH) should count the number of load or store instructions retired. However, due to this erratum, they may undercount.

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

Workaround: None identified.

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

AAJ108. A Page Fault May Not be Generated When the PS bit is set to "1" in a PML4E or PDPTE

Problem: On processors supporting Intel® 64 architecture, the PS bit (Page Size, bit 7) is reserved in PML4Es and PDPTEs. If the translation of the linear address of a memory access encounters a PML4E or a PDPTE with PS set to 1, a page fault should occur. Due to this erratum, PS of such an entry is ignored and no page fault will occur due to its being set.

Implication: Software may not operate properly if it relies on the processor to deliver page faults when reserved bits are set in paging-structure entries.

Workaround: Software should not set bit 7 in any PML4E or PDPTE that has Present Bit (Bit 0) set to "1".

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

**AAJ109. tRP Timing Violations May be Observed Near a Self Refresh Entry**

Problem: When entering package C3, C6 or S3 states, tRP violations may be observed near a self refresh (that is part of the C3, C6 or S3 entry).

Implication: tRP timing violation may occur on DRAM entry to self refresh while entering package C3, C6 or S3 states. Intel has not observed this erratum with any commercially available software. This condition has only been produced in simulation and affects a pre-charge to banks already pre-charged.

Workaround: None identified.

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

AAJ110. System May Hang if MC_CHANNEL_{0,1,2}_MC_DIMM_INIT_CMD.DO_ZQCL Commands Are Not Issued in Increasing Populated DDR3 Rank Order

Problem: ZQCL commands are used during initialization to calibrate DDR3 termination. A ZQCL command can be issued by writing 1 to the MC_CHANNEL_{0,1,2}_MC_DIMM_INIT_CMD.DO_ZQCL (Device 4,5,6, Function 0, Offset 15, bit[15]) field and it targets the DDR3 rank specified in the RANK field (bits[7:5]) of the same register. If the ZQCL commands are not issued in increasing populated rank order then ZQ calibration may not complete, causing the system to hang.

Implication: Due to this erratum the system may hang if writes to the MC_CHANNEL_{0,1,2}_MC_DIMM_INIT_CMD.DO_ZQCL field are not in increasing populated DDR3 rank order.

Workaround: BIOS workaround has been identified. Please refer to the latest version of BIOS Memory Reference Code and release notes.

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

AAJ111. Concurrent Updates to a Segment Descriptor May be Lost

Problem: If a logical processor attempts to set the accessed bit in a code or data segment descriptor while another logical processor is modifying the same descriptor, both modifications of the descriptor may be lost.

Implication: Due to this erratum, updates to segment descriptors may not be preserved. Intel has not observed this erratum with any commercially available software or system.

Workaround: None identified.

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

**AAJ112. Memory Controller Clock Circuits May Show a Temperature Sensitive Dependence on Power-On Conditions**

Problem: A large temperature delta between power-on and run time may affect memory controller clock circuits and subsequently could result in memory errors.

Implication: Correctable/Uncorrectable ECC errors may be observed on a system with memory ECC enabled. On systems that do not have memory ECC enabled, unpredictable system behavior may be observed.

Workaround: It is possible for the BIOS to contain a workaround for this erratum, along with the latest Intel® Tylersburg Platform CPU/QPI/Memory Reference Code.

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

AAJ113. PMIs May be Lost During Core C6 Transitions

Problem: If a performance monitoring counter overflows and causes a PMI (Performance Monitoring Interrupt) at the same time that the core is entering C6, then the PMI may be lost.

Implication: PMIs may be lost during a C6 transition.

Workaround: None identified.

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

AAJ114. Uncacheable Access to a Monitored Address Range May Prevent Future Triggering of the Monitor Hardware

Problem: It is possible that an address range which is being monitored via the MONITOR instruction could be written without triggering the monitor hardware. A read from the monitored address range which is issued as uncacheable (for example having the CR0.CD bit set) may prevent subsequent writes from triggering the monitor hardware. A write to the monitored address range which is issued as uncacheable, may not trigger the monitor hardware and may prevent subsequent writes from triggering the monitor hardware.

Implication: The MWAIT instruction will not exit the optimized power state and resume program flow if the monitor hardware is not triggered.

Workaround: None identified.

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

**AAJ115. BIST Results May be Additionally Reported After a GETSEC[WAKEUP] or INIT-SIPI Sequence**

Problem: BIST results should only be reported in EAX the first time a logical processor wakes up from the Wait-For-SIPI state. Due to this erratum, BIST results may be additionally reported after INIT-SIPI sequences and when waking up RLP's from the SENTER sleep state using the GETSEC[WAKEUP] command.

Implication: An INIT-SIPI sequence may show a non-zero value in EAX upon wakeup when a zero value is expected. RLP's waking up for the SENTER sleep state using the GETSEC[WAKEUP] command may show a different value in EAX upon wakeup than before going into the SENTER sleep state.

Workaround: If necessary software may save the value in EAX prior to launching into the secure environment and restore upon wakeup and/or clear EAX after the INIT-SIPI sequence.

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

AAJ116. 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.

**AAJ117. VM Exits Due to “NMI-Window Exiting” May Be Delayed by One Instruction**

Problem: If VM entry is executed with the “NMI-window exiting” VM-execution control set to 1, a VM exit with exit reason “NMI window” should occur before execution of any instruction if there is no virtual-NMI blocking, no blocking of events by MOV SS, and no blocking of events by STI. If VM entry is made with no virtual-NMI blocking but with blocking of events by either MOV SS or STI, such a VM exit should occur after execution of one instruction in VMX non-root operation. Due to this erratum, the VM exit may be delayed by one additional instruction.

Implication: VMM software using “NMI-window exiting” for NMI virtualization should generally be unaffected, as the erratum causes at most a one-instruction delay in the injection of a virtual NMI, which is virtually asynchronous. The erratum may affect VMMs relying on deterministic delivery of the affected VM exits.

Workaround: None identified.

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

AAJ118. VM Exits Due to EPT Violations Do Not Record Information About Pre-IRET NMI Blocking

Problem: With certain settings of the VM-execution controls VM exits due to EPT violations set bit 12 of the exit qualification if the EPT violation was a result of an execution of the IRET instruction that commenced with non-maskable interrupts (NMIs) blocked. Due to this erratum, such VM exits will instead clear this bit.

Implication: Due to this erratum, a virtual-machine monitor that relies on the proper setting of bit 12 of the exit qualification may deliver NMIs to guest software prematurely.

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.

AAJ119. Multiple Performance Monitor Interrupts are Possible on Overflow of IA32_FIXED_CTR2

Problem: When multiple performance counters are set to generate interrupts on an overflow and more than one counter overflows at the same time, only one interrupt should be generated. However, if one of the counters set to generate an interrupt on overflow is the IA32_FIXED_CTR2 (MSR 30BH) counter, multiple interrupts may be generated when the IA32_FIXED_CTR2 overflows at the same time as any of the other performance counters.

Implication: Multiple counter overflow interrupts may be unexpectedly generated.

Workaround: None identified.

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

**AAJ120. LBRs May Not be Initialized During Power-On Reset of the Processor**

Problem: If a second reset is initiated during the power-on processor reset cycle, the LBRs (Last Branch Records) may not be properly initialized.

Implication: Due to this erratum, debug software may not be able to rely on the LBRs out of power-on reset.

Workaround: Ensure that the processor has completed its power-on reset cycle prior to initiating a second reset.

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

AAJ121. Unexpected Interrupts May Occur on C6 Exit If Using APIC Timer to Generate Interrupts

Problem: If the APIC timer is being used to generate interrupts, unexpected interrupts not related to the APIC timer may be signaled when a core exits the C6 power state. This erratum may occur when the APIC timer is near expiration when entering the core C6 state.

Implication: Due to this erratum, unexpected interrupt vectors could be sent from the APIC to a logical processor.

Workaround: Software should stop the APIC timer (by writing 0 to the Initial Count Register) before allowing the core to enter the C6 state.

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

AAJ122. LBR, BTM or BTS Records May have Incorrect Branch From Information After an EIST Transition, T-states, C1E, or Adaptive Thermal Throttling

Problem: The "From" address associated with the LBR (Last Branch Record), BTM (Branch Trace Message) or BTS (Branch Trace Store) may be incorrect for the first branch after an EIST (Enhanced Intel® SpeedStep Technology) transition, T-states, C1E (C1 Enhanced), or Adaptive Thermal Throttling.

Implication: When the LBRs, BTM or BTS are enabled, some records may have incorrect branch "From" addresses for the first branch after an EIST transition, T-states, C1E, or Adaptive Thermal Throttling.

Workaround: None identified.

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

**AAJ123. Redirection to Probe Mode May be delayed beyond Intended Instruction**

Problem: An attempt to redirect to probe mode (i.e. by hitting hardware breakpoints) may result in a slip of several instructions before the break is taken. This does not impact single-step operation.

Implication: In-Target Probe debug software may not break on the expected instruction.

Workaround: None identified.

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

AAJ124. VMX-Preemption Timer Does Not Count Down at the Rate Specified

Problem: The VMX-preemption timer should count down by 1 every time a specific bit in the TSC (Time Stamp Counter) changes. (This specific bit is indicated by IA32_VMX_MISC bits [4:0] (0x485h) and has a value of 5 on the affected processors.) Due to this erratum, the VMX-preemption timer may instead count down at a different rate and may do so only intermittently.

Implication: The VMX-preemption timer may cause VM exits at a rate different from that expected by software.

Workaround: None identified.

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

AAJ125. Multiple Performance Monitor Interrupts are Possible on Overflow of Fixed Counter 0

Problem: The processor can be configured to issue a PMI (performance monitor interrupt) upon overflow of the IA32_FIXED_CTR0 MSR (309H). A single PMI should be observed on overflow of IA32_FIXED_CTR0, however multiple PMIs are observed when this erratum occurs.

This erratum only occurs when IA32_FIXED_CTR0 overflows and the processor and counter are configured as follows:

- Intel® Hyper-Threading Technology is enabled.
- IA32_FIXED_CTR0 local and global controls are enabled.
- IA32_FIXED_CTR0 is set to count events only on its own thread (IA32_FIXED_CTR_CTRL MSR (38DH) bit [2] = '0').
- PMIs are enabled on IA32_FIXED_CTR0 (IA32_FIXED_CTR_CTRL MSR bit [3] = '1').
- Freeze_on_PMI feature is enabled (IA32_DEBUGCTL MSR (1D9H) bit [12] = '1').

Implication: When this erratum occurs there may be multiple PMIs observed when IA32_FIXED_CTR0 overflows.

Workaround: Disable the FREEZE_PERFMON_ON_PMI feature in IA32_DEBUGCTL MSR (1D9H) bit [12].

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

**AAJ126. VM Exits Due to LIDT/LGDT/SIDT/SGDT Do Not Report Correct Operand Size**

Problem: When a VM exit occurs due to a LIDT, LGDT, SIDT, or SGDT instruction with a 32-bit operand, bit 11 of the VM-exit instruction information field should be set to 1. Due to this erratum, this bit is instead cleared to 0 (indicating a 16-bit operand).

Implication: Virtual-machine monitors cannot rely on bit 11 of the VM-exit instruction information field to determine the operand size of the instruction causing the VM exit.

Workaround: Virtual-machine monitor software may decode the instruction to determine operand size.

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

AAJ127. Performance Monitoring Events STORE_BLOCKS.NOT_STA and STORE_BLOCKS.STA May Not Count Events Correctly

Problem: Performance Monitor Events STORE_BLOCKS.NOT_STA and STORE_BLOCKS.STA should only increment the count when a load is blocked by a store. Due to this erratum, the count will be incremented whenever a load hits a store, whether it is blocked or can forward. In addition this event does not count for specific threads correctly.

Implication: If Intel® Hyper-Threading Technology is disabled, the Performance Monitor events STORE_BLOCKS.NOT_STA and STORE_BLOCKS.STA may indicate a higher occurrence of loads blocked by stores than have actually occurred. If Intel Hyper-Threading Technology is enabled, the counts of loads blocked by stores may be unpredictable and they could be higher or lower than the correct count.

Implication: None identified.

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

AAJ128. Storage of PEBS Record Delayed Following Execution of MOV SS or STI

Problem: When a performance monitoring counter is configured for PEBS (Precise Event Based Sampling), overflow of the counter results in storage of a PEBS record in the PEBS buffer. The information in the PEBS record represents the state of the next instruction to be executed following the counter overflow. Due to this erratum, if the counter overflow occurs after execution of either MOV SS or STI, storage of the PEBS record is delayed by one instruction..

Implication: When this erratum occurs, software may observe storage of the PEBS record being delayed by one instruction following execution of MOV SS or STI. The state information in the PEBS record will also reflect the one instruction delay.

Workaround: None identified.

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

**AAJ129. Performance Monitoring Event FP_MMX_TRANS_TO_MMX May Not Count Some Transitions**

Problem: Performance Monitor Event FP_MMX_TRANS_TO_MMX (Event CCH, Umask 01H) counts transitions from x87 Floating Point (FP) to MMX™ instructions. Due to this erratum, if only a small number of MMX instructions (including EMMS) are executed immediately after the last FP instruction, a FP to MMX transition may not be counted.

Implication: The count value for Performance Monitoring Event FP_MMX_TRANS_TO_MMX may be lower than expected. The degree of undercounting is dependent on the occurrences of the erratum condition while the counter is active. 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.

AAJ130. INVLPG Following INVEPT or INVVPID May Fail to Flush All Translations for a Large Page

Problem: This erratum applies if the address of the memory operand of an INVEPT or INVVPID instruction resides on a page larger than 4KBytes and either (1) that page includes the low 1 MBytes of physical memory; or (2) the physical address of the memory operand matches an MTRR that covers less than 4 MBytes. A subsequent execution of INVLPG that targets the large page and that occurs before the next VM-entry instruction may fail to flush all TLB entries for the page. Such entries may persist in the TLB until the next VM-entry instruction.

Implication: Accesses to the large page between INVLPG and the next VM-entry instruction may incorrectly use translations that are inconsistent with the in-memory page tables.

Workaround: None Identified.

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

**AAJ131. The PECI Bus May be Tri-stated After System Reset**

Problem: During power-up, the processor may improperly assert the PECI (Platform Environment Control Interface) pin. This condition is cleared as soon as Bus Clock starts toggling. However, if the PECI host (also referred to as the master or originator) incorrectly determines this asserted state as another PECI host initiating a transaction, it may release control of the bus resulting in a permanent tri-state condition.

Implication: Due to this erratum, the PECI host may incorrectly determine that it is not the bus master and consequently PECI commands initiated by the PECI software layer may receive incorrect/invalid responses.

Implication: To workaround this erratum the PECI host should pull the PECI bus low to initiate a PECI transaction.

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

AAJ132. LER MSR 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.

AAJ133. An Exit From the Core C6-state May Result in the Dropping of an Interrupt

Problem: In a complex set of internal conditions when the processor exits from Core C6 state, it is possible that an interrupt may be dropped.

Implication: Due to this erratum, an interrupt may be dropped. 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.

AAJ134. PMIs During Core C6 Transitions May Cause the System to Hang

Problem: If a performance monitoring counter overflows and causes a PMI (Performance Monitoring Interrupt) at the same time that the core enters C6, then this may cause the system to hang.

Implication: Due to this erratum, the processor may hang when a PMI coincides with core C6 entry.

Workaround: None identified.

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

**AAJ135. Page Split Lock Accesses Combined With Complex Internal Events May Cause Unpredictable System Behavior**

Problem: A 2MB Page Split Lock (a locked access that spans two 2MB large pages) coincident with additional requests that have particular address relationships in combination with a timing sensitive sequence of complex internal conditions may cause unpredictable system behavior.

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.

AAJ136. IA32_MC8_CTL2 MSR is Not Cleared on Processor Warm Reset

Problem: After processor warm reset the IA32_MC8_CTL2 MSR (288H) should be zero. Due to this erratum the IA32_MC8_CTL2 MSR is not zeroed on processor warm reset.

Implication: When this erratum occurs, the IA32_MC8_CTL2 MSR will not be zeroed by warm reset. Software that expects the values to be 0 coming out of warm reset may not behave as expected.

Workaround: None identified.

Status: BIOS should zero the IA32_MC8_CTL2 MSR after a warm reset.

AAJ137. The Combination of a Page-Split Lock Access And Data Accesses That Are Split Across Cacheline Boundaries May Lead to Processor Livelock

Problem: Under certain complex micro-architectural conditions, the simultaneous occurrence of a page-split lock and several data accesses that are split across cacheline boundaries may lead to processor livelock.

Implication: Due to this erratum, a livelock may occur that can only be terminated by a processor reset. 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.

**AAJ138. FP Data Operand Pointer May Be Incorrectly Calculated After an FP Access Which Wraps a 4-Gbyte Boundary in Code That Uses 32-Bit Address Size in 64-bit Mode**

Problem: The FP (Floating Point) Data Operand Pointer is the effective address of the operand associated with the last non-control FP instruction executed by the processor. If an 80-bit FP access (load or store) occurs in a 16-bit mode other than protected mode (in which case the access will produce a segment limit violation), the memory access wraps a 64-Kbyte boundary, and the FP environment is subsequently saved, the value contained in the FP Data Operand Pointer may be incorrect.

Implication: Due to this erratum, the FP Data Operand Pointer may be incorrect. Wrapping an 80-bit FP load around a 4-Gbyte boundary in this way is not a normal programming practice. Intel has not observed this erratum with any commercially available software.

Workaround: If the FP Data Operand Pointer is used in an operating system which may run 16-bit FP code, care must be taken to ensure that no 80-bit FP accesses are wrapped around a 64-Kbyte boundary.

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

AAJ139. IO_SMI Indication in SMRAM State Save Area May Be Lost

Problem: The IO_SMI bit (bit 0) in the IO state field at SMRAM offset 7FA4H is set to "1" by the processor to indicate a System Management Interrupt (SMI) is either taken immediately after a successful I/O instruction or is taken after a successful iteration of a REP I/O instruction. Due to this erratum, the setting of the IO_SMI bit may be lost. This may happen under a complex set of internal conditions with Intel® Hyper-Threading Technology enabled and has not been observed with commercially available software.

Implication: Due to this erratum, SMI handlers may not be able to identify the occurrence of I/O SMIs.

Workaround: None identified.

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

AAJ140. Performance Monitor Events for Hardware Prefetches Which Miss The L1 Data Cache May be Over Counter

Problem: Hardware prefetches that miss the L1 data cache but cannot be processed immediately due to resource conflicts will count and then retry. This may lead to incorrectly incrementing the L1D_PREFETCH.MISS (event 4EH, umask 02H) event multiple times for a single.

Implication: The count reported by the L1D_PREFETCH.MISS event may be higher than expected.

Workaround: None identified.

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

**AAJ141. VM Exit May Incorrectly Clear IA32_PERF_GLOBAL_CTRL [34:32]**

Problem: If the “load IA32_PERF_GLOBAL_CTRL” VM-exit control is 1, a VM exit should load the IA32_PERF_GLOBAL_CTRL MSR (38FH) from the IA32_PERF_GLOBAL_CTRL field in the guest-state area of the VMCS. Due to this erratum, such a VM exit may instead clear bits 34:32 of the MSR, loading only bits 31:0 from the VMCS.

Implication: All fixed-function performance counters will be disabled after an affected VM exit, even if the VM exit should have enabled them based on the IA32_PERF_GLOBAL_CTRL field in the guest-state area of the VMCS.

Workaround: A VM monitor that wants the fixed-function performance counters to be enabled after a VM exit may do one of two things: (1) clear the “load IA32_PERF_GLOBAL_CTRL” VM-exit control; or (2) include an entry for the IA32_PERF_GLOBAL_CTRL MSR in the VM-exit MSR-load list.

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

AAJ142. QPI Lane May Be Dropped During Full Frequency Deskew Phase of Training

Problem: A random QPI Lane may be dropped during the lane deskew phase while the QPI Bus is training at full frequency.

Implication: When there are multiple resets after the QPI Bus has reached full speed operation there is a small chance that a lane could be dropped during the deskew phase of training. In the case of a lane being dropped this will be detected and a retry will be done until the link is established and the lane is re-trained.

Workaround: None identified.

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

AAJ143. PerfMon Overflow Status Can Not be Cleared After Certain Conditions Have Occurred

Problem: Under very specific timing conditions, if software tries to disable a PerfMon counter through MSR IA32_PERF_GLOBAL_CTRL (0x38F) or through the per-counter event-select (e.g. MSR 0x186) and the counter reached its overflow state very close to that time, then due to this erratum the overflow status indication in MSR IA32_PERF_GLOBAL_STAT (0x38E) may be left set with no way for software to clear it.

Implication: Due to this erratum, software may be unable to clear the PerfMon counter overflow status indication.

Workaround: Software may avoid this erratum by clearing the PerfMon counter value prior to disabling it and then clearing the overflow status indication bit.

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

**AAJ144. An Unexpected Page Fault or EPT Violation May Occur After Another Logical Processor Creates a Valid Translation for a Page**

Problem: An unexpected page fault (#PF) or EPT violation may occur for a page under the following conditions:

- The paging structures initially specify no valid translation for the page.
- Software on one logical processor modifies the paging structures so that there is a valid translation for the page (e.g., by setting to 1 the present bit in one of the paging-structure entries used to translate the page).
- Software on another logical processor observes this modification (e.g., by accessing a linear address on the page or by reading the modified paging-structure entry and seeing value 1 for the present bit).
- Shortly thereafter, software on that other logical processor performs a store to a linear address on the page.

In this case, the store may cause a page fault or EPT violation that indicates that there is no translation for the page (e.g., with bit 0 clear in the page-fault error code, indicating that the fault was caused by a not-present page). Intel has not observed this erratum with any commercially available

Implication: An unexpected page fault may be reported. There are no other side effects due to this erratum.

Workaround: System software can be constructed to tolerate these unexpected page faults. See Section "Propagation of Paging-Structure Changes to Multiple Processors" of Volume 3A of *IA-32 Intel® Architecture Software Developer's Manual*, for recommendations for software treatment of asynchronous paging-structure updates.

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

AAJ145. L1 Data Cache Errors May be Logged With Level Set to 1 Instead of 0

Problem: When an L1 Data Cache error is logged in IA32_MCi_STATUS[15:0], which is the MCA Error Code Field, with a cache error type of the format 0000 0001 RRRR TTLL, the LL field may be incorrectly encoded as 01b instead of 00b.

Implication: An error in the L1 Data Cache may report the same LL value as the L2 Cache. Software should not assume that an LL value of 01b is the L2 Cache.

Workaround: None identified.

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

**AAJ146. Stack Pushes May Not Occur Properly for Events Delivered Immediately After VM Entry to 16-Bit Software**

Problem: Problem: The stack pushes for an event delivered after VM entry and before execution of an instruction in VMX non-root operation may not occur properly. The erratum applies only if the VM entry establishes IA32_EFER.LMA = 0 and CS.D = 0 and only if the event handler is also invoked with CS.D = 0.

Implication: This erratum affects events that are pending upon completion of VM entry and that do not cause VM exits. Examples include debug exceptions, interrupts, and general-protection faults generated in virtual-8086 mode by the mode's virtual interrupt mechanism. The erratum applies only if the VM entry is not to IA-32e mode and is to 16-bit operation, and only if the relevant handler uses 16-bit operation. The incorrect stack pushes resulting from the erratum may cause incorrect guest operation. 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.

AAJ147. PerfMon Event LOAD_HIT_PRE.SW_PREFETCH May Overcount

Problem: PerfMon event LOAD_HIT_PRE.SW_PREFETCH (event 4CH, umask 01H) should count load instructions hitting an ongoing software cache fill request initiated by a preceding software prefetch instruction. Due to this erratum, this event may also count when there is a preceding ongoing cache fill request initiated by a locking instruction.

Implication: PerfMon event LOAD_HIT_PRE.SW_PREFETCH may overcount.

Workaround: None identified.

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

**AAJ148. Successive Fixed Counter Overflows May be Discarded**

Problem: Under specific internal conditions, when using Freeze PerfMon on PMI feature (bit 12 in IA32_DEBUGCTL.Freeze_PerfMon_on_PMI, MSR 1D9H), if two or more PerfMon Fixed Counters overflow very closely to each other, the overflow may be mishandled for some of them. This means that the counter's overflow status bit (in MSR_PERF_GLOBAL_STATUS, MSR 38EH) may not be updated properly; additionally, PMI interrupt may be missed if software programs a counter in Sampling-Mode (PMI bit is set on counter configuration).

Implication: Successive Fixed Counter overflows may be discarded when Freeze PerfMon on PMI is used.

Workaround: Software can avoid this by:

1. Avoid using Freeze PerfMon on PMI bit.
2. Enable only one fixed counter at a time when using Freeze PerfMon on PMINone identified.

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

AAJ149. #GP May be Signaled When Invalid VEX Prefix Precedes Conditional Branch Instructions

Problem: When a 2-byte opcode of a conditional branch (opcodes 0F8xH, for any value of x) instruction resides in 16-bit code-segment and is associated with invalid VEX prefix, it may sometimes signal a #GP fault (illegal instruction length > 15-bytes) instead of a #UD (illegal opcode) fault.

Implication: Due to this erratum, #GP fault instead of a #UD may be signaled on an illegal instruction.

Workaround: None identified.

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

**AAJ150. A Logical Processor May Wake From Shutdown State When Branch-Trace Messages or Branch-Trace Stores Are Enabled**

Problem: Normally, a logical processor that entered the shutdown state will remain in that state until a break event (NMI, SMI, INIT) occurs. Due to this erratum, if CR4.MCE (Machine Check Enable) is 0 and a branch-trace message or branch-trace store is pending at the time of a machine check, the processor may not remain in shutdown state. In addition, if the processor was in VMX non-root operation when it improperly woke from shutdown state, a subsequent VM exit may save a value of 2 into the activity-state field in the VMCS (indicating shutdown) even though the VM exit did not occur while in shutdown state.

Implication: This erratum may result in unexpected system behavior. If a VM exit saved a value of 2 into the activity-state field in the VMCS, the next VM entry will take the processor to shutdown state.

Workaround: None identified.

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

AAJ151. Task Switch to a TSS With an Inaccessible LDTR Descriptor May Cause Unexpected Faults

Problem: A task switch may load the LDTR (Local Descriptor Table Register) with an incorrect segment descriptor if the LDT (Local Descriptor Table) segment selector in the new TSS specifies an inaccessible location in the GDT (Global Descriptor Table).

Implication: Future accesses to the LDT may result in unpredictable system behavior.

Workaround: Operating system code should ensure that segment selectors used during task switches to the GDT specify offsets within the limit of the GDT and that the GDT is fully paged into memory.

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

AAJ152. Changes to Reserved Bits of Some Non-Architectural MSR's May Cause Unpredictable System Behavior

Problem: Under normal circumstances, an operation fails if it attempts to modify a reserved bit of a model-specific register (MSR). Due to this erratum and for some non-architectural MSRs, such an attempt may cause unpredictable system behavior.

Implication: Unpredictable system behavior may occur if software attempts to modify reserved bits of some non-architectural MSRs. (Note that documentation of the WRMSR instruction states that "Undefined or reserved bits in an MSR should be set to values previously read.")

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

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

**AAJ153. VM Entries That Return From SMM Using VMLAUNCH May Not Update The Launch State of the VMCS**

Problem: Successful VM entries using the VMLAUNCH instruction should set the launch state of the VMCS to "launched". Due to this erratum, such a VM entry may not update the launch state of the current VMCS if the VM entry is returning from SMM.

Implication: Subsequent VM entries using the VMRESUME instruction with this VMCS will fail. RFLAGS.ZF is set to 1 and the value 5 (indicating VMRESUME with non-launched VMCS) is stored in the VM-instruction error field. This erratum applies only if dual monitor treatment of SMI and SMM is active.

Workaround: None identified.

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

AAJ154. VM Entry May Clear Bytes 81H-83H on Virtual-APIC Page When "Use TPR Shadow" Is 0

Problem: VM entry should not clear bytes 81H-83H on the virtual-APIC page if the "use TPR shadow" VM-execution control is 0. Due to this erratum, VM entry will do so if the "virtualize x2APIC mode" VM-execution control is 1.

Implication: VM entries with the 0-setting of the "use TPR shadow" VM-execution control and the 1-setting of the "virtualize x2APIC mode" VM-execution control cause any non-zero data at bytes 81H-83H on the virtual-APIC page to be lost. Note that this combination of settings is not allowed; any such VM entry will fail after clearing these bytes.

Workaround: Software should always set the "use TPR shadow" VM-execution control to 1 whenever it sets that "virtualize x2APIC mode" VM-execution control to 1.

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

AAJ155. A First Level Data Cache Parity Error May Result in Unexpected Behavior

Problem: When a load occurs to a first level data cache line resulting in a parity error in close proximity to other software accesses to the same cache line and other locked accesses the processor may exhibit unexpected behavior.

Implication: Due to this erratum unpredictable system behavior may occur. Intel has not observed this erratum with any commercially available system.

Workaround: None identified.

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

**AAJ156. An Event May Intervene Before a System Management Interrupt That Results from IN or INS**

- Problem:** If an I/O instruction (IN, INS, OUT, or OUTS) results in an SMI (system-management interrupt), the processor will set the IO_SMI bit at offset 7FA4H in SMRAM. This interrupt should be delivered immediately after execution of the I/O instruction so that the software handling the SMI can cause the I/O instruction to be re-executed. Due to this erratum, it is possible for another event (e.g., a nonmaskable interrupt) to be delivered before the SMI that follows the execution of an IN or INS instruction.
- Implication:** If software handling an affected SMI uses I/O instruction restart, the handler for the intervening event will not be executed.
- Workaround:** The SMM handler has to evaluate the saved context to determine if the SMI was triggered by an instruction that read from an I/O port. The SMM handler must not restart an I/O instruction if the platform has not been configured to generate a synchronous SMI for the recorded I/O port address.
- Status:** For the steppings affected, see the Summary Table of Change.





Specification Changes

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

- *Intel® Core™ i7 Processor Extreme Edition and Intel® Core™ i7 Processor Datasheet*
- *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*

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





Specification Clarifications

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

- *Intel® Core™ i7 Processor Extreme Edition and Intel® Core™ i7 Processor Datasheet*
- *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*

AAJ1

Clarification of TRANSLATION LOOKASIDE BUFFERS (TLBS) Invalidation

Section 10.9 INVALIDATING THE TRANSLATION LOOKASIDE BUFFERS (TLBS) of the Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A: System Programming Guide will be modified to include the presence of page table structure caches, such as the page directory cache, which Intel processors implement. This information is needed to aid operating systems in managing page table structure invalidations properly.

Intel will update the Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A: System Programming Guide in the coming months. Until that time, an application note, TLBs, Paging-Structure Caches, and Their Invalidation (<http://www.intel.com/products/processor/manuals/index.htm>), is available which provides more information on the paging structure caches and TLB invalidation.

In rare instances, improper TLB invalidation may result in unpredictable system behavior, such as system hangs or incorrect data. Developers of operating systems should take this documentation into account when designing TLB invalidation algorithms. For the processors affected, Intel has provided a recommended update to system and BIOS vendors to incorporate into their BIOS to resolve this issue. The Intel® Core™ i7 processor is not affected by this issue.





Documentation Changes

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

- *Intel® Core™ i7 Processor Extreme Edition and Intel® Core™ i7 Processor Datasheet*
- *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. Follow the link below 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.

