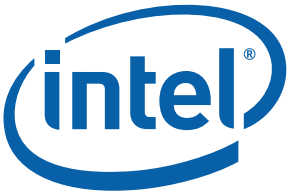


Intel® Core™ i7 Processor Family for LGA2011-v3 Socket

Specification Update

Supporting Desktop Intel® Core™ i7-6950X Extreme Edition Processor for the LGA2011-v3 Socket

Supporting Desktop Intel® Core™ i7-6900K, i7-6850K, and i7-6800K processors for the LGA2011-v3 Socket

January 2017

Revision 002

Reference Number: 334208-002

Contents

Revision History

Version	Description	Date
001	Initial release.	May 2016
002	• Errata — Modified BDH21 — Added BDH68	January 2017

§ §

Preface

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

Information types defined in Nomenclature are consolidated into the specification update and are no longer published in other documents.

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

Affected Documents

Document Title	Document Number/Location
Intel® Core™ i7 Processor Family for LGA2011-v3 Socket Datasheet Volume 1 of 2	334206
Intel® Core™ i7 Processor Family for LGA2011-v3 Socket Datasheet Volume 2 of 2	334207

Related Documents

Document Title	Document Number/ Location
Intel® 64 and IA-32 Architecture Software Developer's Manual • Volume 1: Basic Architecture • Volume 2A: Instruction Set Reference Manual A-M • Volume 2B: Instruction Set Reference Manual N-Z • Volume 3A: System Programming Guide • Volume 3B: System Programming Guide • A-32 Intel® Architecture Optimization Reference Manual	http://www.intel.com/products/processor/manuals/index.htm

Nomenclature

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

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

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

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

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

Identification Information

Component Identification via Programming Interface

The 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	0100b		00b	0110b	1111b	varies per stepping

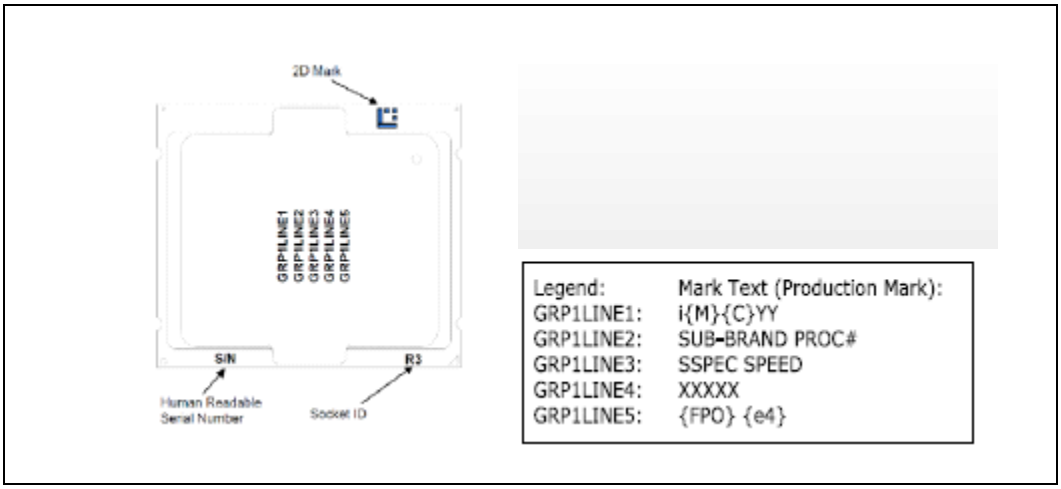
Notes:
1. The Extended Family, Bits [27:20] are used in conjunction with the Family Code, specified in Bits [11:8], to indicate whether the processor belongs to the Intel386™, Intel486™, Pentium®, Pentium 4, or Intel® Core™ processor family.
2. The Extended Model, Bits [19:16] in conjunction with the Model Number, specified in Bits [7:4], are used to identify the model of the processor within the processor's family.
3. The Family Code corresponds to Bits [11:8] of the EDX register after RESET, Bits [11:8] of the EAX register after the CPUID instruction is executed with a 1 in the EAX register, and the generation field of the Device ID register accessible through Boundary Scan.
4. The Model Number corresponds to Bits [7:4] of the EDX register after RESET, Bits [7:4] of the EAX register after the CPUID instruction is executed with a 1 in the EAX register, and the model field of the Device ID register accessible through Boundary Scan.
5. The Stepping ID in Bits [3:0] indicates the revision number of that model. See 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

Figure 1. Processor Top-side Markings (Example)



The processor stepping can be identified by the following component markings. Refer to the Dear Customer Letter (DCL) for additional details and conditions of test support.

Table 1. Processor Family Identification

S-Spec #	Processor Number	Stepping	CPUID	Base Frequency (GHz)	Memory Frequency (MHz)	TDP (W)	# Cores	Cache Size (MB)
R2PA	I7-6950X	R-0	000406F1h	3.0	2400	140	10	25
R2PB	I7-6900K	R-0	000406F1h	3.2	2400	140	8	20
R2PC	I7-6850K	R-0	000406F1h	3.6	2400	140	6	15
R2PD	I7-6800K	R-0	000406F1h	3.4	2400	140	6	15

Summary Tables of Changes

The following tables indicate the errata, specification changes, specification clarifications, or documentation changes which apply to the Product Name 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 uses the following notations:

Codes Used in Summary Tables

Stepping

X:	Errata exists in the stepping indicated. Specification Change or Clarification that applies to this stepping.
(No mark) or (Blank box):	This erratum is fixed in listed stepping or specification change does not apply to listed stepping.

Page

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

Status

Doc:	Document change or update will be implemented.
Plan Fix:	This erratum may be fixed in a future stepping of the product.
Fixed:	This erratum has been previously fixed.
No Fix:	There are no plans to fix this erratum.

Row

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

Table 2. Errata Summary Table (Sheet 1 of 3)

Number	Steppings	Status	ERRATA
	R0		
BDH1	X	No Fix	Enabling ISOCH Mode May Cause The System to Hang
BDH2	X	No Fix	PCI BARs in the Home Agent Will Return Non-Zero Values During Enumeration
BDH3	X	No Fix	PCIe* Header of a Malformed TLP is Logged Incorrectly
BDH4	X	No Fix	A Malformed TLP May Block ECRC Error Logging
BDH5	X	No Fix	The System May Hang During an Intel® QuickPath Interconnect (Intel® QPI) Slow to Fast Mode Transition
BDH6	X	No Fix	PCIe* Header of a Malformed TLP is Logged Incorrectly
BDH7	X	No Fix	Attempting to Enter ADR May Lead to Unpredictable System Behavior
BDH8	X	No Fix	PCI BARs in the Home Agent Will Return Non-Zero Values During Enumeration
BDH9	X	No Fix	The System May Shut Down Unexpectedly During a Warm Reset
BDH10	X	No Fix	CAT May Not Behave as Expected

Table 2. Errata Summary Table (Sheet 2 of 3)

Number	Steppings	Status	ERRATA
	R0		
BDH11	X	No Fix	LBR, BTS, BTM May Report a Wrong Address when an Exception/Interrupt Occurs in 64-bit Mode
BDH12	X	No Fix	EFLAGS Discrepancy on Page Faults and on EPT-Induced VM Exits after a Translation Change
BDH13	X	No Fix	MCi_Status Overflow Bit May Be Incorrectly Set on a Single Instance of a DTLB Error
BDH14	X	No Fix	LER MSRs May Be Unreliable
BDH15	X	No Fix	MONITOR or CLFLUSH on the Local XAPIC's Address Space Results in Hang
BDH16	X	No Fix	#GP on Segment Selector Descriptor that Straddles Canonical Boundary May Not Provide Correct Exception Error Code
BDH17	X	No Fix	FREEZE_WHILE_SMM Does Not Prevent Event From Pending PEBS During SMM
BDH18	X	No Fix	APIC Error "Received Illegal Vector" May be Lost
BDH19	X	No Fix	Performance Monitor Precise Instruction Retired Event May Present Wrong Indications
BDH20	X	No Fix	CR0.CD Is Ignored in VMX Operation
BDH21	X	No Fix	N/A. Erratum has been removed
BDH22	X	No Fix	Execution of VAESIMC or VAESKEYGENASSIST With An Illegal Value for VEX.vvvv May Produce a #NM Exception
BDH23	X	No Fix	Interrupt From Local APIC Timer May Not Be Detectable While Being Delivered
BDH24	X	No Fix	Pending x87 FPU Exceptions (#MF) May be Signaled Earlier Than Expected
BDH25	X	No Fix	DR6.B0-B3 May Not Report All Breakpoints Matched When a MOV/POP SS is Followed by a Store or an MMX Instruction
BDH26	X	No Fix	VEX.L is Not Ignored with VCVT*2SI Instructions
BDH27	X	No Fix	Processor May Livelock During On Demand Clock Modulation
BDH28	X	No Fix	Performance Monitor Events OTHER_ASSISTS.AVX_TO_SSE And OTHER_ASSISTS.SSE_TO_AVX May Over Count
BDH29	X	No Fix	Performance Monitor Event DSB2MITE_SWITCHES.COUNT May Over Count
BDH30	X	No Fix	Timed MWAIT May Use Deadline of a Previous Execution
BDH31	X	No Fix	IA32_VMX_VMCS_ENUM MSR (48AH) Does Not Properly Report The Highest Index Value Used For VMCS Encoding
BDH32	X	No Fix	Incorrect FROM_IP Value For an RTM Abort in BTM or BTS May be Observed
BDH33	X	No Fix	Locked Load Performance Monitoring Events May Under Count
BDH34	X	No Fix	Transactional Abort May Cause an Incorrect Branch Record
BDH35	X	No Fix	PMI May be Signaled More Than Once For Performance Monitor Counter Overflow
BDH36	X	No Fix	Execution of FXSAVE or FXRSTOR With the VEX Prefix May Produce a #NM Exception
BDH37	X	No Fix	VM Exit May Set IA32_EFER.NXE When IA32_MISC_ENABLE Bit 34 is Set to 1
BDH38	X	No Fix	A MOV to CR3 When EPT is Enabled May Lead to an Unexpected Page Fault or an Incorrect Page Translation
BDH39	X	No Fix	Intel® Processor Trace Packet Generation May Stop Sooner Than Expected
BDH40	X	No Fix	PEBS Eventing IP Field May be Incorrect After Not-Taken Branch
BDH41	X	No Fix	Reading The Memory Destination of an Instruction That Begins an HLE Transaction May Return The Original Value
BDH42	X	No Fix	Intel® TSX Instructions Not Available
BDH43	X	No Fix	Performance Monitoring Event INSTR_RETIRED.ALL May Generate Redundant PEBS Records For an Overflow
BDH44	X	No Fix	Reset During PECI Transaction May Cause a Machine Check Exception
BDH45	X	No Fix	Intel® Processor Trace (Intel® PT) MODE.Exec, PIP, and CBR Packets Are Not Generated as Expected

Table 2. Errata Summary Table (Sheet 3 of 3)

Number	Steppings	Status	ERRATA
	R0		
BDH46	X	No Fix	Performance Monitor Instructions Retired Event May Not Count Consistently
BDH47	X	No Fix	General-Purpose Performance Counters May be Inaccurate with Any Thread
BDH48	X	No Fix	An Invalid LBR May Be Recorded Following a Transactional Abort
BDH49	X	No Fix	Executing an RSM Instruction With Intel® Processor Trace Enabled Will Signal a #GP
BDH50	X	No Fix	Intel® Processor Trace PIP May be Unexpectedly Generated
BDH51	X	No Fix	Processor Core Ratio Changes While in Probe Mode May Result in a Hang
BDH52	X	No Fix	Processor Does Not Check IRTE Reserved Bits
BDH53	X	No Fix	PCIe* TPH Request Capability Structure Incorrectly Advertises Device Specific Mode as Supported
BDH54	X	No Fix	Package C3 State or Deeper May Lead to a Reset
BDH55	X	No Fix	VMX-Preemption Timer May Stop Operating When ACC is Enabled
BDH56	X	No Fix	Intel® Advanced Vector Extensions (Intel® AVX) Workloads May Exceed ICCMAX Limits
BDH57	X	No Fix	Writing MSR_ERROR_CONTROL May Cause a #GP
BDH58	X	No Fix	Enabling ACC in VMX Non-Root Operation May Cause System Instability
BDH59	X	No Fix	Performance Monitoring Counters May Produce Incorrect Results for BR_INST_RETIRED Event on Logical Processor.
BDH60	X	No Fix	An APIC Timer Interrupt During Core C6 Entry May be Lost
BDH61	X	No Fix	Processor Instability May Occur When Using The PECI RdIAMSR Command
BDH62	X	No Fix	A #VE May Not Invalidate Cached Translation Information
BDH63	X	No Fix	Package C-state Transitions While Inband PECI Accesses Are in Progress May Cause Performance Degradation
BDH64	X	No Fix	Attempting Concurrent Enabling of Intel® Processor Trace (Intel® PT) With LBR, BTS, or BTM Results in a #GP
BDH65	X	No Fix	A DDR4 C/A Parity Error in Lockstep Mode May Result in a Spurious Uncorrectable Error
BDH66	X	No Fix	PEBS Record May Be Generated After Being Disabled
BDH67	X	No Fix	Software Using Intel® TSX May Behave Unpredictably
BDH68	X	No Fix	An Intel® Hyper-Threading Technology Enabled Processor May Log Internal Parity Errors or Exhibit Unpredictable System Behavior

Specification Changes

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

Specification Clarifications

No.	SPECIFICATION CLARIFICATIONS
	None for this revision of this specification update.

Documentation Changes

No.	DOCUMENTATION CHANGES
	None for this revision of this specification update.

Errata

BDH1 Enabling ISOCH Mode May Cause The System to Hang

Problem: When ISOCH (Isochronous) operation is enabled within BIOS, the system may hang and fail to boot.

Implication: Due to this erratum, the system may hang and fail to boot.

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*.

BDH2 PCI BARs in the Home Agent Will Return Non-Zero Values During Enumeration

Problem: During system initialization the Operating System may access the standard PCI BARs (Base Address Registers). Due to this erratum, accesses to the Home Agent BAR registers (Bus 1; Device 18; Function 0,4; Offsets 0x14-0x24) will return non-zero values.

Implication: The operating system may issue a warning. Intel has not observed any functional failures due to this erratum.

Workaround: None identified.

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

BDH3 PCIe* Header of a Malformed TLP is Logged Incorrectly

Problem: If a PCIe port receives a malformed TLP (Transaction Layer Packet), an error is logged in the UNCERRSTS register (Device 0; Function 0; Offset 14CH and Device 2-3; Function 0-3; Offset 14CH). Due to this erratum, the header of the malformed TLP is logged incorrectly in the HDRLOG register (Device 0; Function 0; Offset 164H and Device 2-3; Function 0-3; Offset 164H).

Implication: The PCIe header of a malformed TLP is not logged correctly.

Workaround: None identified.

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

BDH4 A Malformed TLP May Block ECRC Error Logging

Problem: If a PCIe* port receives a Malformed TLP that also would generate an ECRC Check Failed error, it should report a Malformed TLP error. When Malformed TLP errors are masked, the processor should report the lower-precedence ECRC Check Failed error but, due to this erratum, it does not.

Implication: Software that relies upon ECRC Check Failed error indication may not behave as expected.

Workaround: None identified.

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

BDH5 The System May Hang During an Intel® QuickPath Interconnect (Intel® QPI) Slow to Fast Mode Transition

Problem: During an Intel QPI slow mode to fast mode transition, the LL_STATUS field of the QPIPCSTS register (Bus 0; Device 8,9,10; Function 0; Offset 0xc0) may not be correctly updated to reflect link readiness.

Implication: The system may hang waiting for the QPIPCSTS.LL_STATUS to update.

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*.

BDH6 Unexpected Performance Loss When Turbo Disabled

Problem: When Intel Turbo Boost Technology is disabled by IA32_MISC_ENABLES MSR (416H) TURBO_MODE_DISABLE bit 38, the Ring operating frequency may be below P1 operating frequency.

Implication: Processor performance may be below expectations for P1 operating frequency.

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*.

BDH7 Attempting to Enter ADR May Lead to Unpredictable System Behavior

Problem: Due to this erratum, an attempt to transition the memory subsystem to ADR (Asynchronous DRAM Self Refresh) mode may fail.

Implication: This erratum may lead to 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*.

BDH8 Exiting From Package C3 or Package C6 With DDR4-2133 May Lead to Unpredictable System Behavior

Problem: Due to this erratum, with DDR4-2133 memory, exiting from PC3 (package C3) or PC6 (package C6) state may lead to unpredictable system behavior.

Implication: This erratum may lead to 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*.

BDH9 The System May Shut Down Unexpectedly During a Warm Reset

Problem: Certain complex internal timing conditions present when a warm reset is requested can prevent the orderly completion of in-flight transactions. It is possible under these conditions that the warm reset will fail and trigger a full system shutdown.

Implication: When this erratum occurs, the system will shut down and all machine check error logs will be lost.

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*.

BDH10 CAT May Not Behave as Expected

Problem: Due to this erratum, CAT (Cache Allocation Technology) way enforcement may not behave as configured.

Implication: When this erratum occurs, cache quality of service guarantees may not be met.

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*.

BDH11 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 (0x00007FFFFFFFFFFF) 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 Tables of Changes*.

BDH12 EFLAGS Discrepancy on Page Faults and on EPT-Induced VM Exits after a Translation Change

Problem: 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 Tables of Changes*.

BDH13 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 Tables of Changes*.

BDH14 LER MSRs May Be Unreliable

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

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

Workaround: None Identified.

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

BDH15 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 Tables of Changes*.

BDH16 #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 Tables of Changes*.

BDH17 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 Tables of Changes*.

BDH18 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 Tables of Changes*.

BDH19 Performance Monitor Precise Instruction Retired Event May Present Wrong Indications

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

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

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

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

BDH20 CR0.CD Is Ignored in VMX Operation

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

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

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

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

BDH21 N/A. Erratum has been removed

BDH22 Execution of VAESIMC or VAESKEYGENASSIST With An Illegal Value for VEX.vvvv May Produce a #NM Exception

Problem: The VAESIMC and VAESKEYGENASSIST instructions should produce a #UD (Invalid-Opcode) exception if the value of the vvvv field in the VEX prefix is not 1111b. Due to this erratum, if CR0.TS is "1", the processor may instead produce a #NM (Device-Not-Available) exception.

Implication: Due to this erratum, some undefined instruction encodings may produce a #NM instead of a #UD exception.

Workaround: Software should always set the vvvv field of the VEX prefix to 1111b for instances of the VAESIMC and VAESKEYGENASSIST instructions.

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

BDH23 Interrupt From Local APIC Timer May Not Be Detectable While Being Delivered

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

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

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

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

BDH24 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 Tables of Changes.*

BDH25 DR6.B0-B3 May Not Report All Breakpoints Matched When a MOV/POP SS is Followed by a Store or an MMX Instruction

Problem: Normally, data breakpoints 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 either an MMX instruction that uses a memory addressing mode with an index or a store instruction.

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

Workaround: None identified.

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

BDH26 VEX.L is Not Ignored with VCVT*2SI Instructions

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

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

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

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

BDH27 Processor May Livelock During On Demand Clock Modulation

Problem: The processor may livelock when (1) a processor thread has enabled on demand clock modulation via bit 4 of the IA32_CLOCK_MODULATION MSR (19AH) and the clock modulation duty cycle is set to 12.5% (02H in bits 3:0 of the same MSR), and (2) the other processor thread does not have on demand clock modulation enabled and that thread is executing a stream of instructions with the lock prefix that either split a cacheline or access UC memory.

Implication: Program execution may stall on both threads of the core subject to this erratum.

Workaround: This erratum will not occur if clock modulation is enabled on all threads when using on demand clock modulation or if the duty cycle programmed in the IA32_CLOCK_MODULATION MSR is 18.75% or higher.

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

BDH28 Performance Monitor Events OTHER_ASSISTS.AVX_TO_SSE And OTHER_ASSISTS.SSE_TO_AVX May Over Count

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

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

Workaround: None identified.

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

BDH29 Performance Monitor Event DSB2MITE_SWITCHES.COUNT May Over Count

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

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

Workaround: None identified.

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

BDH30 Timed MWAIT May Use Deadline of a Previous Execution

Problem: A timed MWAIT instruction specifies a TSC deadline for execution resumption. If a wake event causes execution to resume before the deadline is reached, a subsequent timed MWAIT instruction may incorrectly use the deadline of the previous timed MWAIT when that previous deadline is earlier than the new one.

Implication: A timed MWAIT may end earlier than expected.

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.*

BDH31 IA32_VMX_VMCS_ENUM MSR (48AH) Does Not Properly Report The Highest Index Value Used For VMCS Encoding

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

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

Workaround: None identified.

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

BDH32 Incorrect FROM_IP Value For an RTM Abort in BTM or BTS May be Observed

Problem: During RTM (Restricted Transactional Memory) operation when branch tracing is enabled using BTM (Branch Trace Message) or BTS (Branch Trace Store), the incorrect EIP value (From_IP pointer) may be observed for an RTM abort.

Implication: Due to this erratum, the From_IP pointer may be the same as that of the immediately preceding taken branch.

Workaround: None identified.

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

BDH33 Locked Load Performance Monitoring Events May Under Count

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

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

Workaround: None identified.

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

BDH34 Transactional Abort May Cause an Incorrect Branch Record

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

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

Workaround: None identified.

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

BDH35 PMI May be Signaled More Than Once For Performance Monitor Counter Overflow

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

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

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

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

BDH36 Execution of FXSAVE or FXRSTOR With the VEX Prefix May Produce a #NM Exception

Problem: Attempt to use FXSAVE or FXRSTOR with a VEX prefix should produce a #UD (Invalid-Opcode) exception. If either the TS or EM flag bits in CR0 are set, a #NM (device-not-available) exception will be raised instead of #UD exception.

Implication: Due to this erratum a #NM exception may be signaled instead of a #UD exception on an FXSAVE or an FXRSTOR with a VEX prefix.

Workaround: Software should not use FXSAVE or FXRSTOR with the VEX prefix.

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

BDH37 VM Exit May Set IA32_EFER.NXE When IA32_MISC_ENABLE Bit 34 is Set to 1

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

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

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

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

BDH38 A MOV to CR3 When EPT is Enabled May Lead to an Unexpected Page Fault or an Incorrect Page Translation

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

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

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

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

BDH39 Intel® Processor Trace Packet Generation May Stop Sooner Than Expected

Problem: Setting the STOP bit (bit 4) in a Table of Physical Addresses entry directs the processor to stop Intel PT (Processor Trace) packet generation when the associated output region is filled. The processor indicates this has occurred by setting the Stopped bit (bit 5) of IA32_RTIT_STATUS MSR (571H). Due to this erratum, packet generation may stop earlier than expected.

Implication: When this erratum occurs, the OutputOffset field (bits [62:32]) of the IA32_RTIT_OUTPUT_MASK_PTRS MSR (561H) holds a value that is less than the size of the output region which triggered the STOP condition; Intel PT analysis software should not attempt to decode packet data bytes beyond the OutputOffset.

Workaround: None identified.

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

BDH40 PEBS Eventing IP Field May be Incorrect After Not-Taken Branch

Problem: When a PEBS (Precise-Event-Based-Sampling) record is logged immediately after a not-taken conditional branch (Jcc instruction), the Eventing IP field should contain the address of the first byte of the Jcc instruction. Due to this erratum, it may instead contain the address of the instruction preceding the Jcc instruction.

Implication: Performance monitoring software using PEBS may incorrectly attribute PEBS events that occur on a Jcc to the preceding instruction.

Workaround: None identified.

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

BDH41 Reading The Memory Destination of an Instruction That Begins an HLE Transaction May Return The Original Value

Problem: An HLE (Hardware Lock Elision) transactional region begins with an instruction with the XACQUIRE prefix. Due to this erratum, reads from within the transactional region of the memory destination of that instruction may return the value that was in memory before the transactional region began.

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

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

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

BDH42 Intel® TSX Instructions Not Available

Problem: Intel TSX (Intel Transactional Synchronization Extensions) instructions are not supported and not reported by CPUID.

Implication: The Intel TSX feature is not available.

Workaround: None identified.

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

BDH43 Performance Monitoring Event INSTR_RETIRED.ALL May Generate Redundant PEBS Records For an Overflow

Problem: Due to this erratum, the performance monitoring feature PDIR (Precise Distribution of Instructions Retired) for INSTR_RETIRED.ALL (Event C0H; Umask 01H) will generate redundant PEBS (Precise Event Based Sample) records for a counter overflow. This can occur if the lower 6 bits of the performance monitoring counter are not initialized or reset to 0, in the PEBS counter reset field of the DS Buffer Management Area.

Implication: The performance monitor feature PDIR, may generate redundant PEBS records for an overflow.

Workaround: Initialize or reset the counters such that lower 6 bits are 0.

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

BDH44 Reset During PECI Transaction May Cause a Machine Check Exception

Problem: If a PECI transaction is interrupted by a warm reset, it may result in a machine check exception with MCACOD of 0x402.

Implication: When this erratum occurs, the system becomes unresponsive and a machine check will be generated.

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.*

BDH45 Intel® Processor Trace (Intel® PT) MODE.Exec, PIP, and CBR Packets Are Not Generated as Expected

Problem: The Intel® PT MODE.Exec (MODE packet – Execution mode leaf), PIP (Paging Information Packet), and CBR (Core: Bus Ratio) packets are generated at the following PSB+ (Packet Stream Boundary) event rather than at the time of the originating event as expected.

Implication: The decoder may not be able to properly disassemble portions of the binary or interpret portions of the trace because many packets may be generated between the MODE.Exec, PIP, and CBR events and the following PSB+ event.

Workaround: The processor inserts these packets as status packets in the PSB+ block. The decoder may have to skip forward to the next PSB+ block in the trace to obtain the proper updated information to continue decoding.

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

BDH46 Performance Monitor Instructions Retired Event May Not Count Consistently

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

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

Workaround: None identified.

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

BDH47 General-Purpose Performance Counters May be Inaccurate with Any Thread

Problem: The IA32_PMCx MSR (C1H - C8H) general-purpose performance counters may report inaccurate counts when the associated event selection IA32_PERFEVTSELx MSR's (186H - 18DH) AnyThread field (bit 21) is set and either.

Implication: Due to this erratum, IA32_PMCx counters may be inaccurate.

Workaround: None identified.

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

BDH48 An Invalid LBR May Be Recorded Following a Transactional Abort

Problem: Use of Intel® Transactional Synchronization Extensions may result in a transactional abort. If an abort occurs immediately following a branch instruction, an invalid LBR (Last Branch Record) may be recorded before the LBR produced by the abort.

Implication: The invalid LBR may interfere with execution path reconstruction prior to the transactional abort.

Workaround: None identified.

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

BDH49 Executing an RSM Instruction With Intel® Processor Trace Enabled Will Signal a #GP

Problem: Upon delivery of an SMI (System Management Interrupt), the processor saves and then clears TraceEn in the IA32_RTIT_CTL MSR (570H), thus disabling Intel® Processor Trace (Intel® PT). If the SMI handler enables Intel PT and it remains enabled when an RSM instruction is executed, a shutdown event should occur. Due to this erratum, the processor does not shutdown but instead generates a #GP (general-protection exception).

Implication: When this erratum occurs, a #GP will be signaled.

Workaround: If software enables Intel PT in system-management mode, it should disable Intel® PT before executing RSM.

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

BDH50 Intel® Processor Trace PIP May be Unexpectedly Generated

Problem: When Intel® Processor Trace is enabled, PSB+ (Packet Stream Boundary) packets may include a PIP (Paging Information Packet) even though the OS field (bit 2) of IA32_RTIT_CTL MSR (570H) is 0.

Implication: When this erratum occurs, user-mode tracing (indicated by IA32_RTIT_CTL.OS = 0) may include CR3 address information. This may be an undesirable leakage of kernel information.

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

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

BDH51 Processor Core Ratio Changes While in Probe Mode May Result in a Hang

Problem: If a processor core ratio change occurs while the processor is in probe mode, the system may hang.

Implication: Due to this erratum, the processor may hang.

Workaround: None identified. Processor core ratio changes may be disabled to avoid this erratum.

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

BDH52 Processor Does Not Check IRTE Reserved Bits

Problem: As per the Intel® Virtualization Technology for Directed I/O (Intel® VT-d) specification, bits 63:HAW (Host Address Width) of the Posted Interrupt Descriptor Upper Address field in the IRTE (Interrupt Remapping Table Entry) must be checked for a value of 0; violations must be reported as an interrupt-remapping fault. Due to this erratum, hardware does not perform this check and does not signal an interrupt-remapping fault on violations.

Implication: If software improperly programs the reserved address bits of posted interrupt descriptor upper address in the IRTE to a value other than zero, hardware will not detect and report the violation.

Workaround: Software must ensure posted interrupt address bits 63:HAW in the IRTE are zero.

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

BDH53 PCIe* TPH Request Capability Structure Incorrectly Advertises Device Specific Mode as Supported

Problem: The TPH (Transaction layer packet Processing Hints) Requester Capability Structure (PCI Express Extended Capability ID type 0017H) incorrectly reports that Device Specific Mode is supported in its TPH Requester Capability Register (bit 2 at offset 04H in the capability structure).

Implication: The processor supports only No ST (Steering Tag) Mode. The PCI Express Base Specification allows, in this instance, the TPH Requester Capability Structure's TPH Requester Control Register (at offset 08H) bits 2:0 to be hardwired to '000', forcing No ST Mode. Advertising Device Specific Mode but forcing No ST Mode is a violation of the PCI Express Base Specification (and may be reported as a compliance issue). Intel has not observed this erratum to impact the operation of any commercially available system.

Workaround: None identified.

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

BDH54 Package C3 State or Deeper May Lead to a Reset

Problem: Due to this erratum, the processor may reset and signal a Machine Check error with a IA32_MCi_STATUS.MCACOD value of 0400H when in Package C3 state or deeper.

Implication: When this erratum occurs, the processor will reset and report an uncorrectable machine check error.

Workaround: A BIOS code change has been identified and may be implemented as a workaround for this erratum. It is possible for the BIOS to contain a workaround for this erratum

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

BDH55 VMX-Preemption Timer May Stop Operating When ACC is Enabled

Problem: When the MSR_PKG_CST_CONFIG_CONTROL.ACC_Enable bit (MSR E2H, bit 16) is set, the VMX-preemption timer is not decremented in the HLT state.

Implication: When ACC (Autonomous C-State Control) is enabled, the VMX-preemption timer may not cause a VM exit when expected.

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*.

BDH56 Intel® Advanced Vector Extensions (Intel® AVX) Workloads May Exceed ICCMAX Limits

Problem: Intel AVX workloads require a reduced maximum turbo ratio. Due to this erratum, the Intel AVX turbo ratio is higher than expected which may cause the processor to exceed ICCMAX limits and lead to unpredictable system behavior.

Implication: Due to this erratum, the processor may exhibit 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.*

BDH57 Writing MSR_ERROR_CONTROL May Cause a #GP

Problem: A WRMSR that attempts to set MODE1_MEMERROR_REPORT field (bit 1) and/or MEM_CORRERR_LOGGING_DISABLE field (bit 5) of the MSR_ERROR_CONTROL MSR (17FH) may incorrectly cause a #GP (General Protection exception).

Implication: Due to this erratum, if BIOS attempts to change the value of the listed bits, a #GP may occur.

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.*

BDH58 Enabling ACC in VMX Non-Root Operation May Cause System Instability

Problem: ACC (Autonomous C-State Control) is enabled by setting ACC_Enable (bit 16) of MSR_PKG_CST_CONFIG_CONTROL (E2H) to '1'. If ACC is enabled while the processor is in VMX non-root operation, an unexpected VM exit, a machine check, or unpredictable system behavior may result.

Implication: Enabling ACC may lead to system instability.

Workaround: None identified. BIOS should not enable ACC.

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

BDH59 Performance Monitoring Counters May Produce Incorrect Results for BR_INST_RETIRED Event on Logical Processor.

Problem: Performance monitoring event BR_INST_RETIRED (C4H) counts retired branch instructions. Due to this erratum, when operating on logical processor 1 of any core, BR_INST_RETIRED.FAR_BRANCH (Event C4H; Umask 40H) and BR_INST_RETIRED. ALL_BRANCHES (Event C4H; Umask 04H) may count incorrectly. Logical processor 0 of all cores and cores with SMT disabled are not affected by this erratum.

Implication: Due to this erratum, certain performance monitoring event may produce unreliable results when SMT is enabled.

Workaround: None identified.

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

BDH60 An APIC Timer Interrupt During Core C6 Entry May be Lost

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

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

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

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

BDH61 Processor Instability May Occur When Using The PECI RdIAMSR Command

Problem: Under certain circumstances, reading a machine check register using the PECI (Platform Environmental Control Interface) RdIAMSR command may result in a machine check, processor hang or shutdown.

Implication: Machine check, hang or shutdown may be observed when using the PECI RdIAMSR command.

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.*

BDH62 A #VE May Not Invalidate Cached Translation Information

Problem: An EPT (Extended Page Table) violation that causes a #VE (virtualization exception) may not invalidate the guest-physical mappings that were used to translate the guest-physical address that caused the EPT violation.

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 Tables of Changes.*

BDH63 Package C-state Transitions While Inband PECI Accesses Are in Progress May Cause Performance Degradation

Problem: When a Package C-state transition occurs at the same time an inband PECI transaction occurs, PROCHOT# may be incorrectly asserted.

Implication: Incorrect assertion of PROCHOT# reduces the core frequency to the minimum operating frequency of 1.2 GHz resulting in persistent performance degradation.

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.*

BDH64 Attempting Concurrent Enabling of Intel® Processor Trace (Intel® PT) With LBR, BTS, or BTM Results in a #GP

Problem: If LBR (Last Branch Records), BTS (Branch Trace Store), or BTM (Branch Trace Messages) are enabled in the IA32_DEBUGCTL MSR (1D9H), an attempt to enable Intel PT (Intel® Processor Trace) in IA32_RTIT_CTL MSR (570H) results in a #GP (general protection exception). (Note that the BTM enable bit in IA32_DEBUGCTL MSR is named "TR".) Correspondingly, if Intel PT was previously enabled when an attempt is made to enable LBR, BTS, or BTM, a #GP will occur.

Implication: An unexpected #GP may occur when concurrently enabling any one of LBR, BTS, or BTM with Intel PT.

Workaround: None identified.

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

BDH65 A DDR4 C/A Parity Error in Lockstep Mode May Result in a Spurious Uncorrectable Error

Problem: If a memory C/A (Command/Address) parity error occurs while the memory subsystem is configured in lockstep mode then the channel that observed the error will properly log the error but the associated channel in lockstep will incorrectly log an uncorrectable error in its IA32_MCi_STATUS MSR.

Implication: Due to this erratum, incorrect logging of an uncorrectable memory error in IA32_MCi_STATUS may occur.

Workaround: A BIOS code change has been identified.

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

BDH66 PEBS Record May Be Generated After Being Disabled

Problem: A performance monitoring counter may generate a PEBS (Precise Event Based Sampling) record after disabling PEBS or the performance monitoring counter by clearing the corresponding enable bit in IA32_PEBS_ENABLE MSR (3F1H) or IA32_PERF_GLOBAL_CTRL MSR (38FH).

Implication: A PEBS record generated after a VMX transition will store into memory according to the post-transition DS (Debug Store) configuration. These stores may be unexpected if PEBS is not enabled following the transition.

Workaround: It is possible for the BIOS to contain a workaround for this erratum. A software workaround is possible through disallowing PEBS during VMX non-root operation and disabling PEBS prior to VM entry.

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

BDH67 Software Using Intel® TSX May Behave Unpredictably

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

Implication: This erratum may result in unpredictable behavior of the software using TSX.

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.*

BDH68 An Intel® Hyper-Threading Technology Enabled Processor May Log Internal Parity Errors or Exhibit Unpredictable System Behavior

Problem: Under a complex series of microarchitectural events while running Intel Hyper-Threading Technology, a correctable internal parity error may be logged or the system may exhibit unpredictable behavior.

Implication: When this erratum occurs, a correctable error may be logged (IA32_MC0_STATUS.MCACOD=0005H and IA32_MC0_STATUS.MSCOD=0001H) or unpredictable system behavior may occur. Unpredictable system behavior frequently leads to unexpected faults (e.g. #UD, #PF, #GP).

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.*

§ §