Intel® Xeon® E3-1200 v5 Processor Family

Specification Update

September 2023

Revision 040US

Reference Number: 333133-040US

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

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

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

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

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

Intel® Turbo Boost Technology requires a PC with a processor with Intel Turbo Boost Technology capability. Intel Turbo Boost Technology performance varies depending on hardware, software and overall system configuration. Check with your PC manufacturer on whether your system delivers Intel Turbo Boost Technology. For more information, see http://www.intel.com/content/www/us/en/architecture-and-technology/turbo-boost/turbo-boost-technology.html.

Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

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

Intel, the Intel logo, Xeon, Intel Core, Intel SpeedStep, Pentium, and Celeron are trademarks of Intel Corporation or its subsidiaries.

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

Contents

Revision History

Revision	Description	Date
040US	• Revised title and content of SKW190	September 2023
039	• Added errata SKW192, SKW193, and SKW194	September 2022
038	• Added errata SKW190, SKW191	April 2022
037	• Added errata SKW187, SKW188, SKW189	January 2021
036	• Added erratum SKW186	October 2020
035	• Added erratum SKW185	September 2020
034	• Updated erratum SKW173 • Added erratum SKW184	June 2020
033	• Added errata SKW182 and SKW 183	April 2020
032	• Added errata SKW180 and SKW181	March 2020
031	• Added errata SKW174,SKW175, SKW176, SKW 177, SKW 178, SKW179	February 2020
030	• Revised content and title of SKW36 • Added errata SKW172 and SKW173	August 2019
029	• Added erratum SKW171	July 2019
028	• Added errata SKW168, SKW169, SKW170	May 2019
027	• Not available	February 2019
026	• Added erratum SKW167	November 2018
025	• Removed erratum SKW23 • Updated errata SKW35, SKW50, SKW62, SKW160 • Added errata SKW164 - SKW166	October 2018
024	• Added errata SKW162 - SKW163.	August 2018
023	• Updated errata SKW26, SKW161	July 2018
022	• Added errata SKW160 - SKW161.	June 2018
021	• Added errata SKW154 - SKW159.	March 2018
020	• Updated erratum SKW147. • Added errata SKW152 - SKW153.	February 2018
019	• Added erratum SKW151	November 2017
018	• Added errata SKW149 - SKW150	October 2017
017	• Added erratum SKW148	September 2017
016	• Added erratum SKW146 - SKW147	August 2017
015	• Skipped, no updates	NA
014	• Added erratum SKW145	May 2017
013	• Added errata SKW143 - SKW144.	April 2017
012	• Removed erratum SKW2. • Added errata SKW134 - SKW142. • Updated Product Family SKUs Table.	March 2017
011	• Updated erratum SKW124. • Added errata SKW132 - SKW133.	January 2017
010	• Removed erratum SKW115. • Added errata SKW107- SKW131. • Added Specification clarification SKW1.	October 2016

Revision	Description	Date
008-009	- Skipped.	NA
007	- Added errata SKW102- SKW106.	June 2016
006	- Added errata SKW98 - SKW101.	April 2016
005	- Skipped.	NA
004	- Added errata SKW94 - SKW97.	March 2016
003	- Updated SKW57. - Added errata SKW83-SKW93.	February 2016
002.1	- Added Erratum SKW81-82.	January 2016 (Out of cycle)
002	- Updated SKW12. - Updated SKW67. - Added errata SKW77-SKW80. - Corrected Product family SKU table. - Added Specification change SKW1.	December 2015
001	- Initial Release.	November 2015

Preface

This document is an update to the specifications contained in the next table Affected Documents. 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
Intel® Xeon® Processor E3-1200 v5 Product Family Datasheet, Volume 1 of 2	333131
Intel® Xeon® Processor E3-1200 v5 Product Family Datasheet, Volume 2 of 2	333132

Related Documents

Document Title	Document Number/ Location
Intel® 64 and IA-32 Architectures Software Developer's Manual Volume 2A: Instruction Set Reference, A-L -- See Section "AP-485, Intel® Processor Identification and the CPUID Instruction"	http://www.intel.com/design/processor/applnots/241618.htm
Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1: Basic Architecture *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A: Instruction Set Reference, A-L* *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2B: Instruction Set Reference, M-U* *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2C: Instruction Set Reference, V-Z* *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A: System Programming Guide, Part 1* *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B: System Programming Guide, Part 2* *Intel® 64 and IA-32 Architectures Optimization Reference Manual*	http://www.intel.com/products/processor/manuals/index.htm
Intel® 64 and IA-32 Architectures Software Developer's Manuals	http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html
Advanced Configuration Power Interface (ACPI) Specifications	www.acpi.info

Nomenclature

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

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

Qualification Detail Form (QDF) Number Specification Changes are modifications to the current published specifications. These changes will be incorporated in any new release of the specification.

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

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

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

Summary Tables of Changes

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

Codes Used in Summary Tables

Stepping

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

(No mark)

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

Page

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

Status

Doc: Document change or update will be implemented.

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

Fixed: This erratum has been previously fixed.

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

Row

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

Errata (Sheet 1 of 7)

Number	Steppings	Status	ERRATA
	R-0		
SKW1	X	No Fix	Reported Memory Type May Not Be Used to Access the Virtual-Machine Control Structure (VMCS) and Referenced Data Structures
SKW2	X	No Fix	Erratum has been Removed
SKW3	X	No Fix	Execution of VAESIMC or VAESKEYGENASSIST with An Illegal Value for VEX.vvvv May Produce a Device-Not-Available (#NM) Exception
SKW4	X	No Fix	The Corrected Error Count Overflow Bit in IA32_ MC0_STATUS Is Not Updated When The UC Bit Is Set
SKW5	X	No Fix	VM Exit May Set IA32_EFER.NXE When IA32_MISC_ENABLE Bit 34 Is Set to 1
SKW6	X	No Fix	SMRAM State-Save Area Above the 4 GB Boundary May Cause Unpredictable System Behavior

Errata (Sheet 2 of 7)

Number	Steppings	Status	ERRATA
	R-0		
SKW7	X	No Fix	x87 FPU Exception (#MF) May Be Signaled Earlier Than Expected
SKW8	X	No Fix	Incorrect FROM_IP Value For an Restricted Transactional Memory (RTM) Abort in BTM or BTS May Be Observed
SKW9	X	No Fix	DR6 Register May Contain an Incorrect Value When a MOV to SS or POP SS Instruction Is Followed by an XBEGIN Instruction
SKW10	X	No Fix	Opcode Bytes F3 0F BC May Execute As TZCNT Even When TZCNT Not Enumerated by CPUID
SKW11	X	No Fix	PCIe* Root-port Initiated Compliance State Transmitter Equalization Settings May Be Incorrect
SKW12	X	No Fix	The SMSW Instruction May Execute Within an Enclave
SKW13	X	No Fix	Precise Event Based Sampling (PEBS) Record After a WRMSR to IA32_BIOS_UPDT_TRIG May Be Incorrect
SKW14	X	No Fix	Intel® Processor Trace (Intel® PT) TIP.PGD May Not Have Target IP Payload
SKW15	X	No Fix	Operand-Size Override Prefix Causes 64-bit Operand Form of MOVBE Instruction to Cause an #UD
SKW16	X	No Fix	Execution of the FXSAVE or the FXRSTOR With the VEX Prefix May Produce an #NM Exception
SKW17	X	No Fix	WRMSR May Not Clear The Sticky Count Overflow Bit in The IA32_MCi_STATUS MSRs' Corrected Error Count Field
SKW18	X	No Fix	PEBS Eventing IP Field May Be Incorrect After Not-Taken Branch
SKW19	X	No Fix	Debug Exceptions May Be Lost or Misreported Following WRMSR to IA32_BIOS_UPDT_TRIG
SKW20	X	No Fix	Attempts to Retrain a PCIe* Link May Be Ignored
SKW21	X	No Fix	Intel® PT Packet Stream Boundary (PSB)+ Packets May Contain Unexpected Packets
SKW22	X	No Fix	An Advanced Programmable Interrupt Controller (APIC) Timer Interrupt During Core C6 Entry May Be Lost
SKW24	X	No Fix	VM Entry That Clears TraceEn May Generate a FUP
SKW25	X	No Fix	EDRAM Corrected Error Events May Not Be Properly Logged After a Warm Reset
SKW26	X	No Fix	Performance Monitor Event For Outstanding Offcore Requests May Be Incorrect
SKW27	X	No Fix	Processor Instability May Occur When Using the Platform Environmental Control Interface (PECI) RdIAMSR Command
SKW28	X	No Fix	ENCLU[EGETKEY] Ignores KEYREQUEST.MISCMASK
SKW29	X	No Fix	POPCNT Instruction May Take Longer to Execute Than Expected
SKW30	X	No Fix	ENCLU[EREPORT] May Cause a General Protection Exception (#GP) When TARGETINFO.MISCSELECT Is Non-Zero
SKW31	X	No Fix	A VMX Transition Attempting to Load a Non-Existent MSR May Result in a Shutdown
SKW32	X	No Fix	Transitions Out of 64-Bit Mode May Corrupt the x87 FPU Instruction and Data Pointer Registers
SKW33	X	No Fix	Intel® PT FUP May Be Dropped After the OVF
SKW34	X	No Fix	ENCLS[ECREATE] Causes a #GP if Enclave Base Address Is Not Canonical
SKW35	X	No Fix	Data Breakpoint May Not Be Detected on a REP MOVS
SKW36	X	No Fix	Graphics Error: Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d) Hardware May Cache Invalid Entries
SKW37	X	No Fix	PCIe* and DMI Links With Lane Polarity Inversion May Result in Link Failure
SKW38	X	No Fix	PCIe* Expansion ROM Base Address Register May Be Incorrect
SKW39	X	No Fix	PCIe* Perform Equalization May Lead to Link Failure

Errata (Sheet 3 of 7)

Number	Steppings	Status	ERRATA
	R-0		
SKW40	X	No Fix	Two DIMMs Per Channel 2133 MHz DDR4 SODIMM Daisy-Chain Systems with Different Vendors May Hang
SKW41	X	No Fix	ENCLS[EINIT] Instruction May Unexpectedly #GP
SKW42	X	No Fix	Intel® PT OVF Packet May Be Lost if Immediately Preceding a TraceStop
SKW43	X	No Fix	Detecting an Intel® PT Stopped or Error Condition Within an Intel® TSX Region May Result in a System Hang
SKW44	X	No Fix	WRMSR to IA32_BIOS_UPDT_TRIG May Be Counted as Multiple Instructions
SKW45	X	No Fix	The x87 FIP May Be Incorrect
SKW46	X	No Fix	Branch Instructions May Initialize Intel® Memory Protection Extensions (Intel® MPX) Bound Registers Incorrectly
SKW47	X	No Fix	Writing a Non-Canonical Value to an Last Branch Record (LBR) MSR Does Not Signal a #GP When Intel® PT Is Enabled
SKW48	X	No Fix	Processor May Run Intel® Advanced Vector Extensions (Intel® AVX) Code Much Slower Than Expected
SKW49	X	No Fix	Intel® PT Buffer Overflow May Result in Incorrect Packets
SKW50	X	No Fix	Intel® PT PSB+ Packets May Be Omitted on a C6 Transition
SKW51	X	No Fix	IA32_PERF_GLOBAL_STATUS.TRACE_TOPA_PMI Bit Cannot Be Set by Software
SKW52	X	No Fix	Enabling VMX-Preemption Timer Blocks Hardware Duty Cycling (HDC) Operation
SKW53	X	No Fix	ENCLU[EGETKEY] Instruction Ignores MISCMASK Value
SKW54	X	No Fix	Intel® TSX Abort May Result in Unpredictable System Behavior
SKW55	X	No Fix	Use of Prefetch Instructions May Lead to a Violation of Memory Ordering
SKW56	X	No Fix	Code Segment (CS) Limit Violation May Not Be Detected
SKW57	X	No Fix	Last Level Cache Performance Monitoring Events May Be Inaccurate
SKW58	X	No Fix	#GP Occurs Rather Than the Debug Exception (#DB) on Code Page Split Inside an Intel® SGX Enclave
SKW59	X	No Fix	Execution of VAESENCLAST Instruction May Produce a #NM Exception Instead of a #UD Exception
SKW60	X	No Fix	Intel® SGX Enclave Accesses to the APIC-Access Page May Cause APIC-Access VM Exits
SKW61	X	No Fix	CR3 Filtering Does Not Compare Bits [11:5] of CR3 and IA32_RTIT_CR3_MATCH in PAE Paging Mode
SKW62	X	No Fix	Intel® PT PacketEn Change on C-state Wake May Not Generate a TIP Packet
SKW63	X	No Fix	Graphics Configuration May Not Be Correctly Restored After a Package C8 Exit
SKW64	X	No Fix	x87 FDP Value May Be Saved Incorrectly
SKW65	X	No Fix	PECI Frequency Limited to 1 MHz
SKW66	X	No Fix	Processor Graphics IOMMU Unit May Not Mask DMA Remapping Faults
SKW67	X	No Fix	Processor With Intel® SGX Support May Hang During S3 Wake or Power-On Reset
SKW68	X	No Fix	Pending x87 FPU Exceptions (#MF) May Be Signaled Earlier Than Expected
SKW69	X	No Fix	IA Core Ratio Change Coincident With Outstanding Read to the Display Engine (DE) May Cause a System Hang
SKW70	X	No Fix	TSC Is Not Affected by Warm Reset
SKW71	X	No Fix	Intel® PT Buffer Overflow Indication May be Lost if it Immediately Precedes a TraceStop
SKW72	X	No Fix	Intel® PT CYCThresh Value of 13 Is Not Supported
SKW73	X	No Fix	Intel® PT May Drop Some Timing Packets After Entering Thread C3

Errata (Sheet 4 of 7)

Number	Steppings	Status	ERRATA
	R-0		
SKW74	X	No Fix	Underflow and Denormal Conditions During a Vector Dot Product of Packed Single Precision Floating-Point Values (VDPPS) Instruction With YMM Operands May Not Produce The Expected Results
SKW75	X	No Fix	APIC Timer Interrupt May Be Delivered Early
SKW76	X	No Fix	System May Hang When Using Intel® Trusted Execution Technology (Intel® TXT) And Memory That Supports Address Mirroring
SKW77	X	No Fix	Display Flicker May Occur When Both Intel® VT-d And FBC Are Enabled
SKW78	X	No Fix	Certain Processors May be Configured With an Incorrect Thermal Design Power (TDP)
SKW79	X	No Fix	MOVNTDQA From Write Combining (WC) Memory May Pass Earlier MFENCE Instructions
SKW80	X	No Fix	Integrated Audio Codec May Not Be Detected
SKW81	X	No Fix	Processor May Hang or Cause Unpredictable System Behavior
SKW82	X	No Fix	REP MOVS May Not Operate Correctly With Extended Page Table (EPT) Enabled
SKW83	X	No Fix	Ring Frequency Changes May Cause a Machine Check And System Hang
SKW84	X	No Fix	x87 FPU Data Pointer Updated Only For Instructions That Incur Unmasked Exceptions
SKW85	X	No Fix	WRMSR to IA32_BIOS_UPDT_TRIG Concurrent With an Safer Mode Extensions (SMX) SENTER/SEXIT May Result in a System Hang
SKW86	X	No Fix	Incorrect Branch Predicted Bit in BTS/BTM Branch Records
SKW87	X	No Fix	MACHINE_CLEARS.MEMORY_ORDERING Performance Monitoring Event May Undercount
SKW88	X	No Fix	CTR_FRZ May Not Freeze Some Counters
SKW89	X	No Fix	Instructions And Branches Retired Performance Monitoring Events May Overcount
SKW90	X	No Fix	Some OFFCORE_RESPONSE Performance Monitoring Events May Overcount
SKW91	X	No Fix	Using the BIOS to Disable Cores May Lead to a System Hang
SKW92	X	No Fix	#GP After RSM May Push Incorrect RFLAGS Value When Intel® PT is Enabled
SKW93	X	No Fix	Display Flickering May be Observed with Specific eDP Panels
SKW94	X	No Fix	PEBS Record May Be Generated After Being Disabled
SKW95	X	No Fix	Monitor Trap Flag (MTF) VM Exit on XBEGIN Instruction May Save State Incorrectly
SKW96	X	No Fix	Access to Intel® SGX EPC Page in BLOCKED State Is Not Reported as an Intel® SGX-Induced Page Fault
SKW97	X	No Fix	Software Using Intel® TSX May Behave Unpredictably
SKW98	X	No Fix	Digital Thermal Sensor, version 2.0 (DTS2.0) Fan Control Regulation Is Incorrect
SKW99	X	No Fix	Package-C6 Exit Latency May be Higher Than Expected Leading to Display Flicker
SKW100	X	No Fix	PCIe* Ports Do Not Support DLL Link Active Reporting
SKW101	X	No Fix	MOVNTDQA From WC Memory May Pass Earlier Locked Instructions
SKW102	X	No Fix	System May Hang When EDRAM is Enabled And Double Data Rate (DDR) is Operating at 1600 MHz
SKW103	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
SKW104	X	No Fix	Package C3 Exit Latency May Be Longer Than Expected Leading to Display Flicker
SKW105	X	No Fix	Processor DDR VREF Signals May Briefly Exceed JEDEC Spec When Entering S3 State
SKW106	X	No Fix	Uncore Performance Monitoring Counters May be Disabled or Cleared After Package C7
SKW107	X	No Fix	Complex Interactions With Internal Graphics May Impact Processor Responsiveness
SKW108	X	No Fix	#GP on Segment Selector Descriptor that Straddles Canonical Boundary May Not Provide Correct Exception Error Code

Errata (Sheet 5 of 7)

Number	Steppings	Status	ERRATA
	R-0		
SKW109	X	No Fix	Management Component Transport Protocol (MCTP) Header Packets with TAG 0x5 May Be Dropped
SKW110	X	No Fix	Intel® PT Table of Physical Addresses (ToPA) PerfMon Interrupt (PMI) Does Not Freeze Performance Monitoring Counters
SKW111	X	No Fix	Use of VMASKMOV to Store When Using the EPT May Fail
SKW112	X	No Fix	Hardware P-states (HWP)'s Maximum_Performance Value Is Reset to 0xFF
SKW113	X	No Fix	HWP's Guaranteed_Performance Updated Only on Configurable TDP Changes
SKW114	X	No Fix	HWP's Guaranteed_Performance and Relevant Status/Interrupt May be Updated More Than Once Per Second
SKW115	X	No Fix	Removed
SKW116	X	No Fix	Core and/or Ring Frequency May Be Briefly Lower Than Expected After BIOS Completes
SKW117	X	No Fix	Resume Flag (RF) May be Incorrectly Set in The EFLAGS That Is Saved on a Fault in PEBS or BTS
SKW118	X	No Fix	Some Memory Performance Monitoring Events May Produce Incorrect Results When Filtering on Either OS or USR Modes
SKW119	X	No Fix	RING_PERF_LIMIT_REASONS May be Incorrect
SKW120	X	No Fix	The HWP May Generate Thermal Interrupt While Not Enabled
SKW121	X	No Fix	Camera Device Does Not Issue an Message Signaled Interrupts (MSI) When INTx is Enabled
SKW122	X	No Fix	Violations of Intel® SGX Access-Control Requirements Produce #GP Instead of Page Fault (#PF)
SKW123	X	No Fix	PCIe* Graphics (PEG) Advanced Error Reporting (AER) is Not Enabled
SKW124	X	No Fix	Performance Monitoring Counters May Undercount When Using CPL Filtering
SKW125	X	No Fix	SMRAM State-Save Area Above the 4 GB Boundary May Cause Unpredictable System Behavior
SKW126	X	No Fix	Certain Non-Canonical IA32_BNDCFGS Values Will Not Cause VM-Entry Failures
SKW127	X	No Fix	PEBS EventingIP Field May Be Incorrect Under Certain Conditions
SKW128	X	No Fix	Executing a 256 Bit Intel® AVX Instruction May Cause Unpredictable Behavior
SKW129	X	No Fix	An x87 Store Instruction Which Pends Precision Exception (#PE) May Lead to Unexpected Behavior When EPT A/D Is Enabled.
SKW130	X	No Fix	PECI May Not Be Functional After Power On or S3/S4/S5 Resume
SKW131	X	No Fix	A System Hang or Machine Check May Occur When eDRAM Is Enabled
SKW132	X	No Fix	Load Latency Performance Monitoring Facility May Stop Counting
SKW133	X	No Fix	BNDLDX And BNDSTX May Not Signal #GP on Non-Canonical Bound Directory Access
SKW134	X	No Fix	Digital Thermal Sensor (DTS) Temperature Reading May Be Inaccurate on DDR4 systems
SKW135	X	No Fix	Performance Monitoring Load Latency Events May Be Inaccurate For Gather Instructions
SKW136	X	No Fix	IA32_RTIT_CR3_MATCH MSR Bits[11:5] Are Treated As Reserved
SKW137	X	No Fix	APIC Timer Interrupt May Not Be Generated at The Correct Time In TSC-Deadline Mode
SKW138	X	No Fix	Some Bits in MSR_MISC_PWR_MGMT May Be Updated on Writing Illegal Values to This MSR
SKW139	X	No Fix	Unpredictable System Behavior May Occur When System Agent Enhanced Intel® SpeedStep Technology Is Enabled
SKW140	X	No Fix	Processor May Hang Under Complex Scenarios
SKW141	X	No Fix	The Intel® PT CR3 Filter Is Not Re-evaluated on VM Entry

Errata (Sheet 6 of 7)

Number	Steppings	Status	ERRATA
	R-0		
SKW142	X	No Fix	Display Slowness May Be Observed Under Certain Display Commands Scenario
SKW143	X	No Fix	CPUID TLB Associativity Information Is Inaccurate
SKW144	X	No Fix	Short Loops Which Use AH/BH/CH/DH Registers May Cause Unpredictable System Behavior
SKW145	X	No Fix	Processor Graphics May Render Incorrectly or May Hang Following Warm Reset With Package C8 Disabled
SKW146	X	No Fix	Unpredictable System Behavior May Occur in DDR4 Multi-Rank System
SKW147	X	No Fix	Processor May Hang on Complex Sequence of Conditions
SKW148	X	No Fix	Display Artifacts May Be Seen With High Bandwidth, Multiple Display Configurations
SKW149	X	No Fix	Spurious Corrected Errors May Be Reported
SKW150	X	No Fix	Masked Bytes in a Vector Masked Store Instructions May Cause Write Back of a Cache Line
SKW151	X	No Fix	Processor May Incorrectly Assert PROCHOT During PkgC10
SKW152	X	No Fix	Writing Non-Zero Values to Read Only Fields in IA32_THERM_STATUS MSR May #GP
SKW153	X	No Fix	Precise Performance Monitoring May Generate Redundant PEBS Records
SKW154	X	No Fix	Intel® SGX ENCLS[EINIT] May Not Signal an Error For an Incorrectly Formatted SIGSTRUCT Input
SKW155	X	No Fix	Branch Instruction Address May Be Incorrectly Reported on Intel® TSX Abort When Using Intel® MPX
SKW156	X	No Fix	Setting Performance Monitoring IA32_PERF_GLOBAL_STATUS_SET MSR Bit 63 May Not #GP
SKW157	X	No Fix	Hitting a Code Breakpoint Inside a Intel® SGX Debug Enclave May Cause The Processor to Hang
SKW158	X	No Fix	Performance Monitoring Anti Side-Channel Interference (ASCI) Status Bit May be Inaccurate
SKW159	X	No Fix	Processor May Hang When Executing Code In an Hardware Lock Elision (HLE) Transaction Region
SKW160	X	No Fix	Intel® PT CYC Packet Can Be Dropped When Immediately Preceding PSB
SKW161	X	No Fix	Intel® PT VM-entry Indication Depends on The Incorrect VMCS Control Field
SKW162	X	No Fix	VCVTPS2PH To Memory May Update MXCSR in The Case of a Fault on the Store
SKW163	X	No Fix	Intel® PT May Drop All Packets After an Internal Buffer Overflow
SKW164	X	No Fix	ZMM/YMM Registers May Contain Incorrect Values
SKW165	X	No Fix	Intel® PT ToPA Tables Read From Non-Cacheable Memory During an Intel® TSX Transaction May Lead to Processor Hang
SKW166	X	No Fix	Performing an XACQUIRE to an Intel® PT ToPA Table May Lead to Processor Hang
SKW167	X	No Fix	When Virtualization Exceptions are Enabled, EPT Violations May Generate Erroneous Virtualization Exceptions
SKW168	X	No Fix	Using Intel® TSX Instructions May Lead to Unpredictable System Behavior
SKW169	X	No Fix	Performance Monitoring General Purpose Counter 3 May Contain Unexpected Values
SKW170	X	No Fix	Intel® PT Trace May Silently Drop Second Byte of CYC Packet
SKW171	X	No Fix	Unexpected Uncorrected Machine Check Errors May Be Reported
SKW172	X	No Fix	Gen9 Graphics VT-d Hardware May Cache Invalid Entries
SKW173	X	No Fix	A Pending Fixed Interrupt May Be Dispatched Before an Interrupt of The Same Priority Completes
SKW174	X	No Fix	Executing Some Instructions May Cause Unpredictable Behavior

Errata (Sheet 7 of 7)

Number	Steppings	Status	ERRATA
	R-0		
SKW175	X	No Fix	Incorrect Execution of Internal Branch Instructions May Lead to Unpredictable System Behavior
SKW176	X	No Fix	Unexpected Page Faults in Guest Virtualization Environment
SKW177	X	No Fix	Intel® SGX Key Confidentiality May Be Compromised
SKW178	X	No Fix	Instruction Fetch May Cause Machine Check if Page Size Was Changed Without Invalidation
SKW179	X	No Fix	System May Hang Under Complex Conditions
SKW180	X	No Fix	PEG PCIe* Link May Fail to Link When Resuming From PKG-C8
SKW181	X	No Fix	Incorrect Error Correcting Code (ECC) Reporting Following Entry to PKG-C7
SKW182	X	No Fix	PMU MSR_UNC_PERF_FIXED_CTR Is Cleared After Pkg C7 or Deeper
SKW183	X	No Fix	Performance Monitoring General Counter 2 May Have Invalid Value Written When Intel® TSX Is Enabled
SKW184	X	No Fix	Overflow Flag in IA32_MC0_STATUS MSR May Be Incorrectly Set
SKW185	X	No Fix	VERR Instruction Inside VM-entry May Cause DR6 to Contain Incorrect Values
SKW186	X	No Fix	Processor May Hang If Warm Reset Triggers While BIOS Is Initialization
SKW187	X	No Fix	A PMI That Freezes LBRs Can Cause a Duplicate Entry in TOS
SKW188	X	No Fix	Display Intel® VT-d TLB Invalidation during Disabling of Intel® VT-d Translations May Cause Display Corruption or Flickering
SKW189	X	No Fix	MD_CLEAR Operations May Not Properly Overwrite All Buffers
SKW190	X	No Fix	Unexpected Code Breakpoint May Occur
SKW191	X	No Fix	Incorrect MCACOD for L2 MCE
SKW192	X	No Fix	Executing AVX Instructions May Cause a Machine Check Error
SKW193	X	No Fix	PCIe Atomic Operation Completion TLPs May Have Non-Zero Reserved Fields
SKW194	X	No Fix	Call Instruction Wrapping Around The 32-bit Address Boundary May Return to Incorrect Address

Specification Changes

Number	SPECIFICATION CHANGES
SKW1	Intel® Xeon® E3-1235L v5 and E3-1240L v5 processor ICCmax Specification to Change from 40A to 55A.

Specification Clarifications

Number	SPECIFICATION CLARIFICATIONS
SKW1	Attempts to Simultaneously Perform Microcode Updates

Documentation Changes

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

Identification Information

Component Identification Using Programming Interface

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

Table 1. Component Identification

Reserved	Extended Family	Extended Model	Reserved	Processor Type	Family Code	Model Number	Stepping ID
31:28	27:20	19:16	15:14	13:12	11:8	7:4	3:0
▨	00000000b	0101b	▨	00b	0110b	1110b	xxxxb

Notes:

1. The Extended Family, Bits [27:20], is used in conjunction with the Family Code, specified in Bits [11:8], to indicate whether the processor belongs to the Intel® 386™, Intel® 486™, 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], is used to identify the model of the processor within the processor's family.
3. The Family Code corresponds to Bits [11:8] of the Extended Data Register (EDX) register after RESET, Bits [11:8] of the Extended Accumulator Register (EAX) register after the CPUID instruction is executed with a 1 in the EAX register, and the generation field of the Device ID register accessible through Boundary Scan.
4. The Model Number corresponds to Bits [7:4] of the EDX register after RESET, Bits [7:4] of the EAX register after the CPUID instruction is executed with a 1 in the EAX register, and the model field of the Device ID register accessible through Boundary Scan.
5. The Stepping ID in Bits [3:0] indicates the revision number of that model. See the processor Identification table for the processor stepping ID number in the CPUID information.

When EAX is initialized to a value of "1", the CPUID instruction returns the Extended Family, Extended Model, Processor Type, Family Code, Model Number and Stepping ID value in the EAX register. Note that the EDX processor signature value after reset is equivalent to the processor signature output value in the EAX register.

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

The processor can be identified by the following register contents.

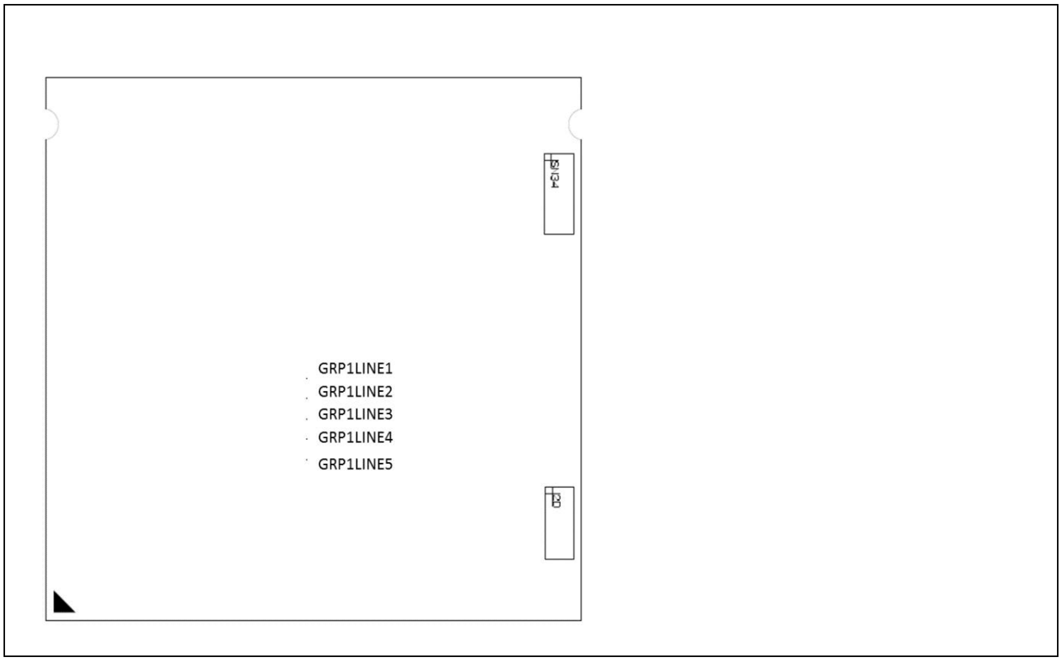
Table 2. Processor Identification by Register Contents

Processor Line	Stepping	Vendor ID	Host Device ID	Processor Graphics Device ID	Host Revision ID	Compatibility Revision ID
Intel® Xeon® E3-1200 v5	R-0	8086h	1918h	1912h	07h	07h

Component Marking Information

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

Figure 1. Intel® Xeon® E3-1200 v5 Processor Family Land Grid Array (LGA) Top-Side Markings



Pin Count: 1151 Package Size: 37.5 mm x 37.5 mm

Sample (SSPEC):

GRP1LINE1:	Intel logo
GRP1LINE2:	BRAND
GRP1LINE3:	PROC#
GRP1LINE4:	SSPEC SPEED

GRP1LINE5: {FPO} {eX}

For Intel® Xeon® Processor E3-1200 v5 Product Family SKUs, see:

https://ark.intel.com/content/www/us/en/ark/products/series/88210/intel-xeon-processor-e3-v5-family.html#@nofilter

Errata

SKW1. Reported Memory Type May Not Be Used to Access the Virtual-Machine Control Structure (VMCS) and Referenced Data Structures

Problem: Bits [53:50] of the `IA32_VMX_BASIC` Model Specific Register (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 Virtual Machine Extension (VMX) access to the VMCS or referenced data structures will instead use the memory type that the Memory-Type Range Registers (MTRR) specify for the physical address of the access.

Implication: Bits [53:50] of the `IA32_VMX_BASIC` MSR report that the Write-Back (WB) 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 Tables of Changes.

SKW2. Erratum has been Removed

SKW3. Execution of VAESIMC or VAESKEYGENASSIST with An Illegal Value for VEX.vvvv May Produce a Device-Not-Available (#NM) Exception

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

SKW4. The Corrected Error Count Overflow Bit in IA32_ MC0_STATUS Is Not Updated When The UC Bit Is Set

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

Implication: The corrected error count overflow indication will be lost if the overflow occurs after an uncorrectable error has been logged.

Workaround: None identified.

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

SKW5. 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.

SKW6. SMRAM State-Save Area Above the 4 GB Boundary May Cause Unpredictable System Behavior

Problem: If the BIOS uses the Resume System Management Mode (RSM) instruction to load the SMBASE register with a value that would cause any part of the SMRAM state-save area to have an address above 4 GBytes, subsequent transitions into and out of System Management Mode (SMM) might save and restore processor state from incorrect addresses.

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

Workaround: Ensure that the SMRAM state-save area is located entirely below the 4 GB address boundary.

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

SKW7. x87 FPU Exception (#MF) May Be Signaled Earlier Than Expected

Problem: x87 instructions that trigger #MF normally service interrupts before the #MF. Due to this erratum, if an instruction that triggers #MF is executing when an Enhanced Intel SpeedStep® Technology transitions, an Intel® Turbo Boost Technology transitions, or a Thermal Monitor event occurs, the #MF may be taken before pending interrupts are serviced.

Implication: Software may observe #MF being signaled before pending interrupts are serviced.

Workaround: None identified.

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

SKW8. Incorrect FROM_IP Value For an Restricted Transactional Memory (RTM) Abort in BTM or BTS May Be Observed

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

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

Workaround: None identified.

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

SKW9. DR6 Register May Contain an Incorrect Value When a MOV to SS or POP SS Instruction Is Followed by an XBEGIN Instruction

Problem: If the XBEGIN is executed immediately after an execution of MOV to SS or PoP SS, a transactional abort occurs and the logical processor restarts execution from the fallback instruction address. If execution of the instruction at that address causes a debug exception, bits [3:0] of the DR6 register may contain an incorrect value.

Implication: When the instruction at the fallback instruction address causes a debug exception, DR6 may report a breakpoint that was not triggered by that instruction, or it may fail to report a breakpoint that was triggered by the instruction.

Workaround: Avoid following a MOV SS or PoP SS instruction immediately with an XBEGIN instruction.

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

SKW10. Opcode Bytes F3 0F BC May Execute As TZCNT Even When TZCNT Not Enumerated by CPUID

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

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

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

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

SKW11. PCIe* Root-port Initiated Compliance State Transmitter Equalization Settings May Be Incorrect

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

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

Workaround: None identified.

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

SKW12. The SMSW Instruction May Execute Within an Enclave

Problem: The SMSW instruction is illegal within an Intel® Software Guard Extensions (Intel® SGX) enclave, and an attempt to execute it within an enclave should result in a #UD. Due to this erratum, the instruction executes normally within an enclave and does not cause a #UD.

Implication: The SMSW instruction provides access to CR0 bits 15:0 and will provide that information inside an enclave. These bits include NE, ET, TS, EM, MP and PE.

Workaround: None identified. If the SMSW execution inside an enclave is unacceptable, system software should not enable Intel® SGX.

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

SKW13. Precise Event Based Sampling (PEBS) Record After a WRMSR to IA32_BIOS_UPDT_TRIG May Be Incorrect

Problem: A PEBS record generated by a WRMSR to `IA32_BIOS_UPDT_TRIG` MSR (79H) may have an incorrect value in the Eventing EIP field if an instruction prefix was used on the WRMSR.

Implication: The Eventing EIP field of the generated PEBS record may be incorrect. Intel has not observed this erratum with any commercially available software.

Workaround: Instruction prefixes have no architecturally-defined function for the WRMSR instruction; instruction prefixes should not be used with the WRMSR instruction.

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

SKW14. Intel® Processor Trace (Intel® PT) TIP.PGD May Not Have Target IP Payload

Problem: When Intel® Processor Trace (Intel® PT) is enabled and a direct unconditional branch clears `IA32_RTIT_STATUS.FilterEn` (MSR 571H, bit 0), due to this erratum, the resulting Target IP Packet.Packet Generation Disable (TIP.PGD) may not have an IP payload with the target IP.

Implication: It may not be possible to tell which instruction in the flow caused the TIP.PGD using only the information in trace packets when this erratum occurs.

Workaround: The Intel® PT trace decoder can compare direct unconditional branch targets in the source with the FilterEn address ranges to determine which branch cleared FilterEn.

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

SKW15. Operand-Size Override Prefix Causes 64-bit Operand Form of MOVBE Instruction to Cause an #UD

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

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

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

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

SKW16. Execution of the FXSAVE or the FXRSTOR With the VEX Prefix May Produce an #NM Exception

Problem: Attempt to use the FXSAVE or the FXRSTOR with a VEX prefix should produce a #UD exception. If either the TS or the EM flag bits in CR0 are set, an #NM exception will be raised instead of the #UD exception.

Implication: Due to this erratum an #NM exception may be signaled instead of an #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.

SKW17. WRMSR May Not Clear The Sticky Count Overflow Bit in The IA32_MCi_STATUS MSRs' Corrected Error Count Field

Problem: The sticky count overflow bit is the most significant bit [bit 52] of the corrected error count field (bits [52:38]) in `IA32_MCi_STATUS` MSRs. Once set, the sticky count overflow bit may not be cleared by a WRMSR instruction. When this occurs, that bit can only be cleared by power-on reset.

Implication: Software that uses the corrected error count field and expects to be able to clear the sticky count overflow bit may misinterpret the number of corrected errors when the sticky count overflow bit is set. This erratum does not affect threshold-based Corrected Machine Check Error Interrupt (CMCI) signaling.

Workaround: None identified.

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

SKW18. PEBS Eventing IP Field May Be Incorrect After Not-Taken Branch

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

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

Workaround: None identified.

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

SKW19. Debug Exceptions May Be Lost or Misreported Following WRMSR to IA32_BIOS_UPDT_TRIG

Problem: If the WRMSR instruction writes to the `IA32_BIOS_UPDT_TRIG` MSR (79H) immediately after an execution of MOV SS or PoP SS that generated a debug exception, the processor may fail to deliver the debug exception or, if it does, the DR6 register contents may not correctly reflect the causes of the debug exception.

Implication: Debugging software may fail to operate properly if a debug exception is lost or does not report complete information.

Workaround: Software should avoid using WRMSR instruction immediately after executing MOV SS or PoP SS.

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

SKW20. Attempts to Retrain a PCIe* Link May Be Ignored

Problem: A PCIe* link should retrain when retrain link [bit 5] in the link control register (Bus 0; Device 1; Functions 0,1,2; Offset 0xB0) is set. Due to this erratum, if the link is in the L1 state, it may ignore the retrain request.

Implication: The PCIe* link may not behave as expected.

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

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

SKW21. Intel® PT Packet Stream Boundary (PSB)+ Packets May Contain Unexpected Packets

Problem: Some Intel® PT packets should be issued only between Target IP Packet.Packet Generation Enable (TIP.PGE) and TIP.PGD packets. Due to this erratum, when a TIP.PGE packet is generated it may be preceded by a PSB+ that incorrectly includes Flow Update Packet (FUP) and MODE.Exec packets.

Implication: Due to this erratum, the FUP and the MODE.Exec may be generated unexpectedly.

Workaround: Decoders should ignore the FUP and the MODE.Exec packets that are not between TIP.PGE and TIP.PGD packets.

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

SKW22. An Advanced Programmable Interrupt Controller (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.

SKW24. VM Entry That Clears TraceEn May Generate a FUP

Problem: If the VM entry clears the Intel® PT `IA32_RTIT_CTL.TraceEn` (MSR 570H, bit 0) while PacketEn is 1 then a FUP will precede the TIP.PGD. The VM entry can clear TraceEn if the VM-entry MSR-load area includes an entry for the `IA32_RTIT_CTL` MSR.

Implication: When this erratum occurs, an unexpected FUP may be generated that creates the appearance of an asynchronous event taking place immediately before or during the VM entry.

Workaround: The Intel® PT trace decoder may opt to ignore any FUP whose IP matches that of a VM entry instruction.

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

SKW25. EDRAM Corrected Error Events May Not Be Properly Logged After a Warm Reset

Problem: After a warm reset, an Embedded DRAM (EDRAM) corrected error may not be logged correctly until the associated machine check register is initialized. This erratum may affect `IA32_MC8_STATUS` or `IA32_MC10_STATUS`.

Implication: The EDRAM corrected error information may be lost when this erratum occurs.

Workaround: Data from the affected machine check registers should be read and the registers initialized as soon as practical after a warm reset.

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

SKW26. Performance Monitor Event For Outstanding Offcore Requests May Be Incorrect

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

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

Workaround: None identified.

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

SKW27. Processor Instability May Occur When Using the Platform Environmental Control Interface (PECI) RdIAMSR Command

Problem: Under certain circumstances, reading a machine check register using the PECI 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.

SKW28. ENCLU[EGETKEY] Ignores KEYREQUEST.MISCMASK

Problem: The Intel® SGX ENCLU[EGETKEY] instruction ignores the MISCMASK field in KEYREQUEST structure when computing a provisioning key, a provisioning seal key, or a seal key.

Implication: ENCLU[EGETKEY] will return the same key in response to two requests that differ only in the value of KEYREQUEST.MISCMASK. Intel has not observed this erratum with any commercially available software.

Workaround: When executing the ENCLU[EGETKEY] instruction, software should ensure that the bits set in KEYREQUEST.MISCMASK are a subset of the bits set in the current SECS' MISCSELECT field.

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

SKW29. POPCNT Instruction May Take Longer to Execute Than Expected

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

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

Workaround: None identified.

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

SKW30. ENCLU[EREPORT] May Cause a General Protection Exception (#GP) When TARGETINFO.MISCSELECT Is Non-Zero

Problem: The Intel® SGX ENCLU[EREPORT] instruction may cause a #GP if any bit is set in TARGETINFO structure's MISCSELECT field.

Implication: This erratum may cause unexpected general-protection exceptions inside enclaves.

Workaround: When executing the ENCLU[EREPORT] instruction, software should ensure the bits set in TARGETINFO.MISCSELECT are a subset of the bits set in the current SECS' MISCSELECT field.

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

SKW31. A VMX Transition Attempting to Load a Non-Existent MSR May Result in a Shutdown

Problem: A VMX transition may result in a shutdown (without generating a machine-check event) if a non-existent MSR is included in the associated MSR load area. When such a shutdown occurs, a machine check error will be logged with `IA32_MCi_STATUS.MCACOD` (bits [15:0]) of 406H, but the processor does not issue the special shutdown cycle. A hardware reset must be used to restart the processor.

Implication: Due to this erratum, the hypervisor may experience an unexpected shutdown.

Workaround: Software should not configure VMX transitions to load non-existent MSRs.

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

SKW32. Transitions Out of 64-Bit Mode May Corrupt the x87 FPU Instruction and Data Pointer Registers

Problem: A transition from 64-bit mode to compatibility mode may zero bits [63:32] of the x87 FPU Instruction Pointer (FIP) Offset and the x87 FPU Data Pointer (FDP) Offset .

Implication: A later instruction that saves x87 FPU state will not save bits [63:32] of the instruction and data pointers of the last non-control instruction executed.

Workaround: 64-bit software should save x87 FPU state before leaving 64-bit mode.

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

SKW33. Intel® PT FUP May Be Dropped After the OVF

Problem: Some Intel® PT Overflow (OVF) packets may not be followed by a FUP or TIP.PGE.

Implication: When this erratum occurs, an unexpected packet sequence is generated.

Workaround: When it encounters an OVF without a following FUP or TIP.PGE, the Intel® PT trace decoder should scan for the next TIP, TIP.PGE, or PSB+ to resume operation.

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

SKW34. ENCLS[ECREATE] Causes a #GP if Enclave Base Address Is Not Canonical

Problem: The ENCLS[ECREATE] instruction uses an SECS (Intel® SGX enclave control structure) referenced by the SRCPAGE pointer in the PAGEINFO structure, which is referenced by the RBX register. Due to this erratum, the instruction causes a #GP if the SECS attributes indicate that the enclave should operate in 64-bit mode and the enclave base linear address in the SECS is not canonical.

Implication: System software will incur a general-protection fault if it mistakenly programs the SECS with a non-canonical address. Intel has not observed this erratum with any commercially available software.

Workaround: System software should always specify a canonical address as the base address of the 64-bit mode enclave.

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

SKW35. Data Breakpoint May Not Be Detected on a REP MOVS

Problem: A REP MOVS instruction that causes an exception or a VM exit may not detect a data breakpoint that occurred on an earlier memory access of that REP MOVS instruction.

Implication: A debugger may miss a data read/write access if it is done by a REP MOVS instruction.

Workaround: Software that relies on data breakpoint for correct execution should disable fast-strings (bit 0 in `IA32_MISC_ENABLE` MSR).

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

SKW36. Graphics Error: Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d) Hardware May Cache Invalid Entries

Problem: The processor's graphics I/O Memory Management Unit (IOMMU) may cache invalid Intel® VT-d context entries. This violates the Intel® VT-d specification for HW Caching Mode where hardware implementations of this architecture must not cache invalid entries.

Implication: Due to this erratum, unpredictable system behavior and/or a system hang may occur.

Workaround: Software should flush the Gfx Intel® VT-d context cache after any update of context table entries.

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

SKW37. PCIe* and DMI Links With Lane Polarity Inversion May Result in Link Failure

Problem: The processor's PCIe* and DMI links may fail after exiting Package C7 or deeper if the platform requires the link to utilize lane polarity inversion.

Implication: Due to this erratum, the processor cannot support lane polarity inversion on the PCIe* or DMI links when Package C7 or deeper is enabled.

Workaround: None identified.

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

SKW38. PCIe* Expansion ROM Base Address Register May Be Incorrect

Problem: After PCIe* 8.0 GT/s Link Equalization on a root port (Bus 0; Device 1; Function 0, 1, 2) has completed, the Expansion ROM Base Address Register (Offset 38H) may be incorrect.

Implication: Software that uses this BAR may behave unexpectedly. Intel has not observed this erratum with any commercially available software.

Workaround: It is possible for the BIOS to contain a partial workaround for this erratum. Software should wait at least 5 ms following link equalization before accessing these Expansion ROM Base Address Register.

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

SKW39. PCIe* Perform Equalization May Lead to Link Failure

Problem: Due to this erratum, when a processor PCIe* port operating at 8.0 GT/s is directed to redo equalization, either via software or from the link partner, incorrect coefficients may be conveyed during Equalization Phase 3.

Implication: If the link partner accepts the incorrect coefficients, the link may become unstable. Note this affects 8.0 GT/s only.

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.

SKW40. Two DIMMs Per Channel 2133 MHz DDR4 SODIMM Daisy-Chain Systems with Different Vendors May Hang

Problem: When on a single memory channel with 2133 MHz DDR4 SODIMMs, mixing different vendors or mixing single rank and dual rank DIMMs may lead to a higher rate of correctable errors or system hangs.

Implication: Due to this erratum, reported correctable error counts may increase, or the system may hang.

Workaround: Use a single vendor for and do not mix single rank and dual rank 2133 MHz DDR4 SODIMM.

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

SKW41. ENCLS[EINIT] Instruction May Unexpectedly #GP

Problem: When using Intel® SGX, the ENCLS[EINIT] instruction will incorrectly cause a #GP if the MISCSELECT field of the SIGSTRUCT structure is not zero.

Implication: This erratum may cause an unexpected #GP, but only if software has set bits in the MISCSELECT field in SIGSTRUCT structure that do not correspond to extended features that can be written to the MISC region of the State Save Area (SSA). Intel has not observed this erratum with any commercially available software.

Workaround: When executing the ENCLS[EINIT] instruction, software should only set bits in the MISCSELECT field in the SIGSTRUCT structure that are enumerated as 1 by CPUID.(EAX=12H,ECX=0):EBX (the bit vector of extended features that can be written to the MISC region of the SSA).

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

SKW42. Intel® PT OVF Packet May Be Lost if Immediately Preceding a TraceStop

Problem: If an Intel® PT internal buffer overflow occurs immediately before software executes a taken branch or event that enters an Intel® PT Trace Stop region, the OVF packet may be lost.

Implication: The trace decoder will not see the OVF packet, nor any subsequent packets (for example, TraceStop) that were lost due to overflow.

Workaround: None identified.

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

SKW43. Detecting an Intel® PT Stopped or Error Condition Within an Intel® TSX Region May Result in a System Hang

Problem: While executing within an Intel® TSX transactional region with Intel® PT enabled and an event occurs that causes either the Error bit [bit 4] or Stopped bit [bit 5] in the IA32_RTIT_STATUS MSR (0571H) to be set then, due to this erratum, the system may hang.

Implication: A system hang may occur when Intel® PT and Intel® TSX are used together.

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.

SKW44. WRMSR to IA32_BIOS_UPDT_TRIG May Be Counted as Multiple Instructions

Problem: When software loads a microcode update by writing to MSR IA32_BIOS_UPDT_TRIG (79H) on multiple logical processors in parallel, a logical processor may, due to this erratum, count the WRMSR instruction as multiple instruction-retired events.

Implication: Performance monitoring with the instruction-retired event may over count by up to four extra events per instance of WRMSR which targets the IA32_BIOS_UPDT_TRIG register.

Workaround: None identified.

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

SKW45. The x87 FIP May Be Incorrect

Problem: The x87 FPU should update the x87 FIP for every non-control x87 instruction executed. Due to this erratum, the FIP is valid only if the last non-control FP instruction had an unmasked exception.

Implication: When this erratum occurs, an instruction that saves FIP (for example, FSTENV) may save an incorrect value. Software that depends on the FIP value for x87 non-control instructions without unmasked exceptions may not operate as 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.

SKW46. Branch Instructions May Initialize Intel® Memory Protection Extensions (Intel® MPX) Bound Registers Incorrectly

Problem: Depending on the current Intel® MPX configuration, execution of certain branch instructions (near CALL, near RET, near JMP, and Jcc instructions) without a BND prefix (F2H) initializes the Intel® MPX bound registers. Due to this erratum, execution of such a branch instruction on a user-mode page may not use the Intel® MPX configuration register appropriately to the current privilege level (BNDCFGU for CPL 3 or BNDCFGS otherwise) for determining whether to initialize the bound registers; it may, thus, initialize the bound registers when it should not, or fail to initialize them when it should.

Implication: After a branch instruction on a user-mode page has been executed, a Bound-Range (#BR) exception may occur when it should not have, or a #BR may not occur when one should have.

Workaround: If supervisor software is not expected to execute instructions on user-mode pages, software can avoid this erratum by setting CR4.SMEP[bit 20] to enable Supervisor-Mode Execution Prevention (SMEP). If the SMEP is not available or if supervisor software is expected to execute instructions on user-mode pages, no workaround is identified.

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

SKW47. Writing a Non-Canonical Value to an Last Branch Record (LBR) MSR Does Not Signal a #GP When Intel® PT Is Enabled

Problem: If Intel® PT is enabled, WRMSR will not cause a general-protection exception (#GP) on an attempt to write a non-canonical value to any of the following MSRs:

- `MSR_LASTBRANCH_{0 - 31}_FROM_IP (680H - 69FH)`
- `MSR_LASTBRANCH__{0 - 31}_TO_IP (6C0H - 6DFH)`
- `MSR_LASTBRANCH_FROM_IP (1DBH)`
- `MSR_LASTBRANCH_TO_IP (1DCH)`
- `MSR_LASTINT_FROM_IP (1DDH)`
- `MSR_LASTINT_TO_IP (1DEH)`

Instead the same behavior will occur as if a canonical value had been written. Specifically, the WRMSR will be dropped and the MSR value will not be changed.

Implication: Due to this erratum, an expected #GP may not be signaled.

Workaround: None identified.

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

SKW48. Processor May Run Intel® Advanced Vector Extensions (Intel® AVX) Code Much Slower Than Expected

Problem: After a C6 state exit, the execution rate of Intel® AVX instructions may be reduced.

Implication: Applications using Intel® AVX instructions may run slower 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.

SKW49. Intel® PT Buffer Overflow May Result in Incorrect Packets

Problem: Under complex microarchitectural conditions, an Intel® PT OVF packet may be issued after the first byte of a multi-byte Cycle Count (CYC) packet, instead of any remaining bytes of the CYC.

Implication: When this erratum occurs, the splicing of the CYC and the OVF packets may prevent the Intel® PT decoder from recognizing the overflow. The Intel® PT decoder may then encounter subsequent packets that are not consistent with expected behavior.

Workaround: None identified. The decoder may be able to recognize that this erratum has occurred when a two-byte CYC packet is followed by a single byte CYC, where the latter 2 bytes are 0xf302, and where the CYC packets are followed by a FUP and a PSB+. It should then treat the two CYC packets as indicating an overflow.

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

SKW50. Intel® PT PSB+ Packets May Be Omitted on a C6 Transition

Problem: An Intel® PT PSB+ set of packets may not be generated as expected when IA32_RTIT_STATUS.PacketByteCnt [48:32] (MSR 0x571) reaches the PSB threshold and a logical processor C6 entry occurs within the following one KByte of trace output.

Implication: After a logical processor enters C6, Intel® PT output may be missing PSB+ sets of packets.

Workaround: None identified.

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

SKW51. IA32_PERF_GLOBAL_STATUS.TRACE_TOPA_PMI Bit Cannot Be Set by Software

Problem: A WRMSR that attempts to set Trace_ToPA_PMI (bit 55) in the IA32_PERF_GLOBAL_STATUS MSR (38EH) by writing a 1 to bit 55 in the IA32_PERF_GLOBAL_STATUS_SET (MSR (391H) will cause a #GP fault.

Implication: Software cannot set the Trace_ToPA_PMI bit.

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.

SKW52. Enabling VMX-Preemption Timer Blocks Hardware Duty Cycling (HDC) Operation

Problem: The HDC will not put the physical package into the forced idle state while any logical processor is in VMX non-root operation and the “activate VMX-preemption timer” VM-execution control is 1.

Implication: HDC will not provide the desired power reduction when the VMX-preemption timer is active in VMX non-root operation.

Workaround: None identified.

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

SKW53. ENCLU[EGETKEY] Instruction Ignores MISCMASK Value

Problem: The ENCLU[EGETKEY] instruction always generates SEAL, PROVISION, and PROVISION_SEAL keys as if the MISCMASK field in the KEYREQUEST structure is 0.

Implication: The ENCLU[EGETKEY] instruction will generate the same keys for different MISCMASK values.

Workaround: Software should not rely on ENCLU[EGETKEY] to produce different keys by supplying different MISCMASK values. Software should use other KEYREQUEST fields to produce separation of the keys.

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

SKW54. Intel® TSX Abort May Result in Unpredictable System Behavior

Problem: Certain microarchitectural conditions during an Intel® TSX abort may result in unpredictable system behavior.

Implication: Software using Intel® TSX may be unreliable.

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

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

SKW55. Use of Prefetch Instructions May Lead to a Violation of Memory Ordering

Problem: Under certain micro architectural conditions, execution of a PREFETCHh instruction or a PREFETCHW instruction may cause a load from the prefetched cache line to appear to execute before an earlier load from another cache line.

Implication: Software that relies on loads executing in program order may not operate correctly.

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

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

SKW56. Code Segment (CS) Limit Violation May Not Be Detected

Problem: A CS limit reduction may not be properly applied.

Implication: Instructions may be executed beyond the CS limit. Intel has not observed this erratum to impact the operation of 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 Tables of Changes.

SKW57. Last Level Cache Performance Monitoring Events May Be Inaccurate

Problem: The performance monitoring events `LONGEST_LAT_CACHE.REFERENCE` (Event 2EH; Umask 4FH) and `LONGEST_LAT_CACHE.MISS` (Event 2EH; Umask 41H) count requests that reference or miss in the last level cache. However, due to this erratum, the count may be incorrect.

Implication: `LONGEST_LAT_CACHE` events may be incorrect.

Workaround: None identified. Software may use the following `OFFCORE_REQUESTS` model-specific sub events that provide related performance monitoring data: `DEMAND_DATA_RD`, `DEMAND_CODE_RD`, `DEMAND_RFO`, `ALL_DATA_RD`, `L3_MISS_DEMAND_DATA_RD`, `ALL_REQUESTS`.

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

SKW58. #GP Occurs Rather Than the Debug Exception (#DB) on Code Page Split Inside an Intel® SGX Enclave

Problem: When executing within an Intel® SGX enclave, a #GP may be delivered instead of a #DB when an instruction breakpoint is detected. This occurs when the instruction to be executed spans two pages, the second of which has an entry in the Enclave Page Cache Map (EPCM) that is not valid.

Implication: Debugging software may not be invoked when an instruction breakpoint is detected.

Workaround: Software should ensure that all pages containing enclave instructions have valid EPCM entries.

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

SKW59. Execution of VAESENCLAST Instruction May Produce a #NM Exception Instead of a #UD Exception

Problem: Execution of VAESENCLAST with VEX.L= 1 should signal a #UD exception; however, due to the erratum, a Device Not Available (#NM) exception may be signaled.

Implication: As a result of this erratum, an operating system may restore Intel® AVX and other state unnecessarily.

Workaround: None identified.

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

SKW60. Intel® SGX Enclave Accesses to the APIC-Access Page May Cause APIC-Access VM Exits

Problem: In VMX non-root operation, Intel® SGX enclave accesses to the APIC-access page may cause APIC-access VM exits instead of page faults.

Implication: A VMM may receive a VM exit due to an access that should have caused a page fault, which would be handled by the guest OS.

Workaround: A VMM avoids this erratum if it does not map any part of the Enclave Page Cache (EPC) to the guest’s APIC-access address. An operating system avoids this erratum if it does not attempt indirect enclave accesses to the APIC.

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

SKW61. CR3 Filtering Does Not Compare Bits [11:5] of CR3 and IA32_RTIT_CR3_MATCH in PAE Paging Mode

Problem: In PAE paging mode, the CR3[11:5] are used to locate the page-directory-pointer table. Due to this erratum, those bits of CR3 are not compared to `IA32_RTIT_CR3_MATCH` (MSR 572H) when `IA32_RTIT_CTL.CR3Filter` (MSR 570H, bit 7) is set.

Implication: If multiple page-directory-pointer tables are co-located within a 4 KB region, CR3 filtering will not be able to distinguish between them, so additional processes may be traced.

Workaround: None identified.

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

SKW62. Intel® PT PacketEn Change on C-state Wake May Not Generate a TIP Packet

Problem: A TIP.PGE or TIP.PGD packet may not be generated if Intel® PT PacketEn changes after `IA32_RTIT_STATUS.FilterEn` (MSR 571H, bit 0) is re-evaluated on wakeup from C6 or deeper sleep state.

Implication: When code enters or exits an IP filter region without a taken branch, tracing may begin or cease without proper indication in the trace output. This may affect trace decoder behavior.

Workaround: None identified. A trace decoder will need to skip ahead to the next TIP or FUP packet to determine the current IP.

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

SKW63. Graphics Configuration May Not Be Correctly Restored After a Package C8 Exit

Problem: The processor should ensure internal graphics configuration is restored during a Package C8 or deeper exit event. Due to this erratum, some internal graphics configurations may not be correctly restored.

Implication: When this erratum occurs, a graphics driver restart may lead to system instability. Such a restart may occur when upgrading the graphics driver.

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.

SKW64. x87 FDP Value May Be Saved Incorrectly

Problem: Execution of the FSAVE, FNSAVE, FSTENV, or FNSTENV instructions in real-address mode or virtual-8086 mode may save an incorrect value for the x87 FPU Data Pointer (FDP). This erratum does not apply if the last non-control x87 instruction had an unmasked exception.

Implication: Software operating in real-address mode or virtual-8086 mode that depends on the FDP value for non-control x87 instructions without unmasked exceptions may not operate properly.

Workaround: None identified. Software should use the FDP value saved by the listed instructions only when the most recent non-control x87 instruction incurred an unmasked exception.

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

SKW65. PECI Frequency Limited to 1 MHz

Problem: The PECI 3.1 specification’s operating frequency range is 0.2 MHz to 2 MHz. Due to this erratum, PECI may be unreliable when operated above 1 MHz.

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

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

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

SKW66. Processor Graphics IOMMU Unit May Not Mask DMA Remapping Faults

Problem: Intel® VT-d specification specifies setting the FPD field in the context (or extended-context) entry of IOMMU to mask recording of qualified DMA remapping faults for DMA requests processed through that context entry. Due to this erratum, the IOMMU unit for Processor Graphics device may record DMA remapping faults from Processor Graphics device (Bus: 0; Device: 2; Function: 0) even when the FPD field is set to 1.

Implication: Software may continue to observe DMA remapping faults recorded in the IOMMU Fault Recording Register even after setting the FPD field.

Workaround: None identified. Software may mask the fault reporting event by setting the Interrupt Mask (IM) field in the IOMMU Fault Event Control register (Offset 038H in GFXVTBAR).

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

SKW67. Processor With Intel® SGX Support May Hang During S3 Wake or Power-On Reset

Problem: Processors that support Intel® SGX may experience hangs when waking from S3 (Standby) system sleep state or during a power-on reset. This erratum may occur even if the Intel® SGX feature is not enabled.

Implication: Due to this erratum, the system may not wake after entering standby sleep state or may not start up after a power-on reset

Workaround: It is possible for the BIOS to contain a workaround for this erratum. For systems that do not power gate Vcc Sustain, if the workaround detects this erratum, support for Intel® SGX will be removed until platform power is disconnected and reapplied.

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

SKW68. 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.

SKW69. IA Core Ratio Change Coincident With Outstanding Read to the Display Engine (DE) May Cause a System Hang

Problem: An outstanding read from an IA core to the DE that is coincident with an IA core ratio change 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 Tables of Changes.

SKW70. TSC Is Not Affected by Warm Reset

Problem: The TSC (`IA32_TIME_STAMP_COUNTER` MSR 10H) should be cleared on reset. Due to this erratum, the TSC is not affected by warm reset.

Implication: The TSC is not cleared by a warm reset. The TSC is cleared by power-on reset as expected.

Workaround: None identified.

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

SKW71. Intel® PT Buffer Overflow Indication May be Lost if it Immediately Precedes a TraceStop

Problem: If an Intel® PT internal buffer overflow occurs just before software executes a taken branch or event that enters an Intel® PT TraceStop region, the OVF packet may be lost.

Implication: When this erratum occurs, the decoder will not see the OVF packet or any TIP.PGD (Target IP – Packet Generation Disabled) and may not see the TraceStop packet at the end of the trace.

Workaround: None identified.

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

SKW72. Intel® PT CYCThresh Value of 13 Is Not Supported

Problem: Intel® PT CYC threshold is configured through CYCThresh field in bits [22:19] of `IA32_RTIT_CTL` MSR (570H). A value of 13 is advertised as supported by CPUID (leaf 14H, sub-lead 1H). Due to this erratum, if CYCThresh is set to 13, then the CYC threshold will be 0 cycles instead of 4096 (213-1) cycles.

Implication: CYC packets may be issued in higher rate than expected if threshold value of 13 is used.

Workaround: None identified. Software should not use value of 13 for CYC threshold.

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

SKW73. Intel® PT May Drop Some Timing Packets After Entering Thread C3

Problem: Intel® PT may temporarily stop sending Mini Time Counter (MTC) and CYC packets after entering thread C3 state. MTC and CYC packets may be missing in up to 1KB of trace output after entering thread C3.

Implication: Some Intel® PT timing packets may temporarily not be sent after thread C3 is entered.

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.

SKW74. Underflow and Denormal Conditions During a Vector Dot Product of Packed Single Precision Floating-Point Values (VDPPS) Instruction With YMM Operands May Not Produce The Expected Results

Problem: A VDPPS instruction operating on YMM registers with denormal operands or experiencing an underflow may not produce the expected result if the exception is masked in the MXCSR. This may also happen when intermediate multiply results have underflow conditions.

Implication: VDPPS with YMM registers may not produce the expected result.

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.

SKW75. APIC Timer Interrupt May Be Delivered Early

Problem: When the APIC timer is configured to TSC Deadline Mode, a timer interrupt may occur before the expected deadline if any of IA32_TSC_DEADLINE MSR (6E0H) bits [63:56] are set.

Implication: A timer interrupt may be delivered earlier than specified by the IA32_TSC_DEADLINE MSR.

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.

SKW76. System May Hang When Using Intel® Trusted Execution Technology (Intel® TXT) And Memory That Supports Address Mirroring

Problem: Within platforms that utilize memory that supports address mirroring, processors that utilize Intel® TXT measured launch environment may fail to boot and hang.

Implication: Due to this erratum, system may hang.

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

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

SKW77. Display Flicker May Occur When Both Intel® VT-d And FBC Are Enabled

Problem: Display flickering may occur when both Frame Buffer Compression (FBC) and Intel® VT-d are enabled and in use by the display controller.

Implication: Due to this erratum, display flickering may be observed.

Workaround: It is possible for the graphics driver to contain a workaround for this erratum. This workaround will disable FBC.

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

SKW78. Certain Processors May be Configured With an Incorrect Thermal Design Power (TDP)

Problem: Certain processors should be configured with a TDP limit of 54 or 51 watts. Due to this erratum, these processors may be incorrectly configured at 65 W TDP. The following processors are affected by this erratum: Intel® Core™ i3 Processor Series, Celeron® and Pentium® (Dual-Core With GT1/GT2). A processor that reports a value of 0x208 in TDP_POWER_OF_SKU field in MSR PACKAGE_POWER_SKU (MSR 614H [14:0]) are affected by this erratum.

Implication: Processors affected by this erratum may spend more time in turbo and thus may experience unexpected thermal throttling events.

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.

SKW79. MOVNTDQA From Write Combining (WC) Memory May Pass Earlier MFENCE Instructions

Problem: An execution of MOVNTDQA or VMOVNTDQA that loads from WC memory may appear to pass an earlier execution of the MFENCE instruction.

Implication: When this erratum occurs, an execution of MOVNTDQA or VMOVNTDQA may appear to execute before memory operations that precede the earlier MFENCE instruction. Software that uses MFENCE to order subsequent executions of the MOVNTDQA instructions may not operate properly.

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.

SKW80. Integrated Audio Codec May Not Be Detected

Problem: Integrated Audio Codec may lose power when Low-Power Single Pipe (LPSP) mode is enabled for HDMI ports. Platforms with Intel® Smart Sound Technology (Intel® SST) enabled are not affected.

Implication: The Audio Bus driver may attempt to do enumeration of Codecs when eDP or HDMI port enters LPSP mode. Due to this erratum, the Integrated Audio Codec will not be detected and audio may be lost.

Workaround: Intel® Graphics Driver 15.40.11.4308 or later will prevent the Integrated Audio Codec from losing power when LPSP mode is enabled.

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

SKW81. Processor May Hang or Cause Unpredictable System Behavior

Problem: Under complex microarchitecture conditions, processor may hang with an internal timeout error (MCACOD 0400H) logged into `IA32_MCi_STATUS` or cause unpredictable system behavior.

Implication: When this issue occurs, the system 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 Tables of Changes.

SKW82. REP MOVS May Not Operate Correctly With Extended Page Table (EPT) Enabled

Problem: Execution of REP MOVS may incorrectly change [R/E]CX, [R/E]SI, and/or [R/E]DI register values during instruction execution. This erratum occurs only if the execution would set an accessed or dirty flag in a paging structure to which EPT does not allow writes.

Implication: Incorrect changes to RCX, RSI, and/or RDI may lead to a block-copy operation with an unexpected length, an unexpected source location, and/or an unexpected destination location.

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.

SKW83. Ring Frequency Changes May Cause a Machine Check And System Hang

Problem: Ring frequency changes may lead to a system hang with the processor logging a machine check in IA32_MCi_STATUS where the MCACOD (bits [15:0]) value is 0x0402 and the MSCOD (bits [31:16]) value is 0x77yy (yy is any 8-bit value).

Implication: When this erratum occurs, the system will log a machine check and hang. Power management activity, including system power state changes, can result in ring frequency changes that may trigger 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.

SKW84. x87 FPU Data Pointer Updated Only For Instructions That Incur Unmasked Exceptions

Problem: The x87 FPU data pointer points to the data (operand) for the last x87 non-control instruction executed unless CPUID.(EAX=07H,ECX=0H):EBX.FDP_EXCPTN_ONLY [bit 6] is 1, in which case it points to the operand for the last x87 non-control instruction that incurred an unmasked x87 exception. Due to this erratum, x87 FPU data pointer behaves as if the FDP_EXCPTN_ONLY flag is 1 even when that bit is 0.

Implication: If the most recent x87 non-control instruction did not incur an unmasked x87 exception, software that then examines the x87 FPU data pointer will see an incorrect value. 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 Tables of Changes.

SKW85. WRMSR to IA32_BIOS_UPDT_TRIG Concurrent With an Safer Mode Extensions (SMX) SENTER/SEXIT May Result in a System Hang

Problem: Performing WRMSR to IA32_BIOS_UPDT_TRIG (MSR 79H) on a logical processor while another logical processor is executing an SMX SENTER/SEXIT operation (GETSEC[SENTER] or GETSEC[SEXIT] instruction) may cause the processor to hang.

Implication: When this erratum occurs, the system will hang. Intel has not observed this erratum with any commercially available system.

Workaround: None identified.

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

SKW86. Incorrect Branch Predicted Bit in BTS/BTM Branch Records

Problem: The BTS and the BTM send branch records to the Debug Store management area and system bus respectively. The Branch Predicted bit (bit 4 of eighth byte in BTS/BTM records) should report whether the most recent branch was predicted correctly. Due to this erratum, the branch predicted bit may be incorrect.

Implication: The BTS and the BTM cannot be used to determine the accuracy of branch prediction.

Workaround: None identified.

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

SKW87. MACHINE_CLEARS.MEMORY_ORDERING Performance Monitoring Event May Undercount

Problem: The performance monitoring event MACHINE_CLEARS.MEMORY_ORDERING (Event C3H; Umask 02H) counts the number of machine clears caused by memory ordering conflicts. However due to this erratum, this event may undercount for VGATHER/ VPGATHER instructions with four or more elements.

Implication: MACHINE_CLEARS.MEMORY_ORDERING performance monitoring event may undercount.

Workaround: None identified.

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

SKW88. CTR_FRZ May Not Freeze Some Counters

Problem: IA32_PERF_GLOBAL_STATUS.CTR_FRZ (MSR 38EH, bit 59) is set when either (1) IA32_DEBUGCTL.FREEZE_PERFMON_ON_PMI (MSR 1D9H, bit 12) is set and a Performance Monitor Interrupt (PMI) is triggered, or (2) software sets bit 59 of IA32_PERF_GLOBAL_STATUS_SET (MSR 391H). When set, CTR_FRZ should stop all core performance monitoring counters from counting. However, due to this erratum, IA32_PMC4-7 (MSR C5-C8H) may not stop counting. IA32_PMC4-7 are only available when a processor core is not shared by two logical processors.

Implication: General performance monitoring counters 4-7 may not freeze when IA32_PERF_GLOBAL_STATUS.CTR_FRZ is set.

Workaround: None identified.

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

SKW89. Instructions And Branches Retired Performance Monitoring Events May Overcount

Problem: The performance monitoring events INST_RETIRED (Event C0H; any Umask value) and BR_INST_RETIRED (Event C4H; any Umask value) count instructions retired and branches retired, respectively. However, due to this erratum, these events may overcount in certain conditions when:

- Executing VMASKMOV instructions with at least one masked vector element
- Executing REP MOVS or REP STOS with Fast Strings enabled (IA32_MISC_ENABLES MSR (1A0H), bit 0 set)
- An Intel® MPX #BR exception occurs on BNDLDX/BNDSTX instructions and the BR_INST_RETIRED (Event C4H; Umask is 00H or 04H) is used.

Implication: INST_RETIRED and BR_INST_RETIRED performance monitoring events may overcount.

Workaround: None identified.

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

SKW90. Some OFFCORE_RESPONSE Performance Monitoring Events May Overcount

Problem: The performance monitoring events OFFCORE_RESPONSE (events B7H and BBH) should count off-core responses matching the request-response configuration specified in MSR_OFFCORE_RSP_0 and MSR_OFFCORE_RSP_1 (1A6H and 1A7H, respectively) for core-originated requests. However, due to this erratum, DMND_RFO (bit 1), DMND_IFETCH (bit 2) and OTHER (bit 15) request types may overcount.

Implication: Some OFFCORE_RESPONSE events may overcount.

Workaround: None identified. Software may use the following model-specific events that provide related performance monitoring data: OFFCORE_REQUESTS (all sub-events), L2_TRANS.L2_WB and L2_RQSTS.PF_MISS.

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

SKW91. Using the BIOS to Disable Cores May Lead to a System Hang

Problem: Using the BIOS hardware core disable facility may cause the processor to hang when it attempts to enter or exit Package C6.

Implication: When this erratum occurs, attempting to enter or exit Package C6 state will hang the system.

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

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

SKW92. #GP After RSM May Push Incorrect RFLAGS Value When Intel® PT is Enabled

Problem: If Intel® PT is enabled, a #GP caused by the instruction fetch immediately following execution of an RSM instruction may push an incorrect value for RFLAGS onto the stack.

Implication: Software that relies on the RFLAGS value pushed on the stack under the conditions described may not work properly.

Workaround: None identified.

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

SKW93. Display Flickering May be Observed with Specific eDP Panels

Problem: The processor may incorrectly configure transmitter buffer characteristics if the associated embedded Display Port (eDP) panel requests VESA equalization preset three, five, six, or eight.

Implication: Display flickering or display loss maybe observed.

Workaround: Graphics Driver version 15.40.12.4326 or later contains a workaround for this erratum.

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

SKW94. PEBS Record May Be Generated After Being Disabled

Problem: A performance monitoring counter may generate a PEBS record after disabling the 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 configuration. These stores may be unexpected if the 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.

SKW95. Monitor Trap Flag (MTF) VM Exit on XBEGIN Instruction May Save State Incorrectly

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

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

Workaround: None identified.

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

SKW96. Access to Intel® SGX EPC Page in BLOCKED State Is Not Reported as an Intel® SGX-Induced Page Fault

Problem: If a page fault results from an attempt to access a page in the Intel® SGX EPC that is in the BLOCKED state, the processor does not indicate that the page fault was Intel® SGX induced by setting bit 15 of the error code pushed on the stack.

Implication: Due to this erratum, software may not recognize these page faults as being Intel® SGX induced.

Workaround: Before using the EBLOCK instruction to marking a page as BLOCKED, software should mark the page not present.

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

SKW97. Software Using Intel® TSX May Behave Unpredictably

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

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

SKW98. Digital Thermal Sensor, version 2.0 (DTS2.0) Fan Control Regulation Is Incorrect

Problem: The DTS2.0 fan control temperature is incorrect.

Implication: Due to this erratum, the incorrect fan control temperature may lead to the processor running hot enough to reach its thermal throttling point, unnecessarily reducing processor performance. Other thermal control methods are not impacted by 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.

SKW99. Package-C6 Exit Latency May be Higher Than Expected Leading to Display Flicker

Problem: Package-C6 exit latency may be higher than expected.

Implication: Due to this erratum, the display may flicker or other Isochronous devices may be affected.

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.

SKW100. PCIe* Ports Do Not Support DLL Link Active Reporting

Problem: The PCIe* Base Specification requires every "Downstream Port that supports Link speeds greater than 5.0 GT/s" to support Data Link Layer (DLL) Link Active Reporting, However, the PCIe* ports do not support DLL Link Active Reporting.

Implication: Due to this erratum, the PCIe* ports do not support DLL Link Active Reporting. This may be reported by a PCIe* compliance test.

Workaround: None identified.

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

SKW101. MOVNTDQA From WC Memory May Pass Earlier Locked Instructions

Problem: An execution of (V)MOVNTDQA (streaming load instruction) that loads from the WC memory may appear to pass an earlier locked instruction that accesses a different cache line.

Implication: Software that expects a lock to fence subsequent (V)MOVNTDQA instructions may not operate properly.

Workaround: None identified. Software that relies on a locked instruction to fence subsequent executions of (V)MOVNTDQA should insert an MFENCE instruction between the locked instruction and subsequent (V)MOVNTDQA instruction.

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

SKW102. System May Hang When EDRAM is Enabled And Double Data Rate (DDR) is Operating at 1600 MHz

Problem: When EDRAM is enabled and the DDR operating frequency is 1600 MHz, a system hang may occur.

Implication: When this erratum occurs, 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.

SKW103. 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.

SKW104. Package C3 Exit Latency May Be Longer Than Expected Leading to Display Flicker

Problem: Package C3 exit latency may be longer than expected.

Implication: When this erratum occurs on a system with multiple high resolution displays, the displays may flicker.

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.

SKW105. Processor DDR VREF Signals May Briefly Exceed JEDEC Spec When Entering S3 State

Problem: Voltage glitch of up to 200 mV on the VREF signal lasting for about 1 mS may be observed when entering System S3 state. This violates the JEDEC Double Data Rate (DDR) specifications

Implication: 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.

SKW106. Uncore Performance Monitoring Counters May be Disabled or Cleared After Package C7

Problem: After entering into Package C7, the following Uncore performance monitoring MSRs may be cleared to zero: MSR_ UNC _PERF_GLOBAL_CTRL (E01H), MSR_ UNC _PERF_GLOBAL_STATUS (E02H), MSR_ UNC _PERF_FIXED_CTRL (394H), MSR_ UNC _PERF_FIXED_CTR (395H).

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

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

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

SKW107. Complex Interactions With Internal Graphics May Impact Processor Responsiveness

Problem: Under complex conditions associated with the use of internal graphics, the processor may exceed the MAX_LAT CSR values (PCI configuration space, offset 03FH, bits[7:0]).

Implication: When this erratum occurs, the processor responsiveness is affected. 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.

SKW108. #GP on Segment Selector Descriptor that Straddles Canonical Boundary May Not Provide Correct Exception Error Code

Problem: During a #GP, 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.

SKW109. Management Component Transport Protocol (MCTP) Header Packets with TAG 0x5 May Be Dropped

Problem: Downstream MCTP packets from the processor to the PCH will be incorrectly routed during MCTP device enumeration if the TAG field of the MCTP message header has a value of 0x5 and the routing type is Route to Root Complex (Type=0).

Implication: The device will function but cannot be MCTP managed. This issue has only been observed with a synthetic test device where the MCTP header field was set to 0x5.

Workaround: MCTP devices should not use a TAG of 0x5 when performing MCTP enumeration.

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

SKW110. Intel® PT Table of Physical Addresses (ToPA) PerfMon Interrupt (PMI) Does Not Freeze Performance Monitoring Counters

Problem: Due to this erratum, if `IA32_DEBUGCTL.FREEZE_PERFMON_ON_PMI (MSR 1D9H, bit 12)` is set to 1 when Intel® PT triggers a ToPA PMI, performance monitoring counters are not frozen as expected.

Implication: Performance monitoring counters will continue to count for events that occur during PMI handler execution.

Workaround: PMI handler software can programmatically stop performance monitoring counters upon entry.

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

SKW111. Use of VMASKMOV to Store When Using the EPT May Fail

Problem: Use of VMASKMOV instructions to store data that splits over two pages, when the instruction resides on the first page may cause a hang if the EPT is in use, and the store to the second page requires setting the A/D bits in the EPT entry.

Implication: Due to this erratum, the CPU may hang on the execution of VMASKMOV.

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.

SKW112. Hardware P-states (HWP)'s Maximum_Performance Value Is Reset to 0xFF

Problem: According to HWP specification, the reset value of the `Maximum_Performance` field (bits [15:8]) in `IA32_HWP_REQUEST` MSR (774h) should be set to the value of `IA32_HWP_CAPABILITIES` MSR (771H) `Highest_Performance` field (bits [7:0]) after reset. Due to this erratum, the reset value of Maximum_Performance is always set to 0xFF.

Implication: Software may see an unexpected value in the Maximum Performance field. Hardware clipping will prevent invalid performance states.

Workaround: None identified.

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

SKW113. HWP's Guaranteed_Performance Updated Only on Configurable TDP Changes

Problem: According to HWP specification, the Guaranteed_Performance field (bits [15:8]) in the `IA32_HWP_CAPABILITIES` MSR (771H) should be updated as a result of changes in the configuration of TDP, Running Average Power Limit (RAPL), RATL and other platform tuning options that may have dynamic effects on the actual guaranteed performance support level. Due to this erratum, the processor will update the `Guaranteed_Performance` field only as a result of configurable TDP dynamic changes.

Implication: Software may read a stale value of the `Guaranteed _Performance` field.

Workaround: None identified.

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

SKW114. HWP's Guaranteed_Performance and Relevant Status/Interrupt May be Updated More Than Once Per Second

Problem: According to HWP specification, the `Guaranteed_Performance` field (bits [15:8]) in the `IA32_HWP_CAPABILITIES` MSR (771H) and the Guaranteed_Performance_Change (bit 0) bit in `IA32_HWP_STATUS` MSR (777H) should not be changed more than once per second nor should the thermal interrupt associated with the change to these fields be signaled more than once per second. Due to this erratum, the processor may change these fields and generate the associated interrupt more than once per second.

Implication: HWP interrupt rate due to the `Guaranteed_Performance` field change can be higher than specified.

Workaround: Clearing the `Guaranteed_Performance_Change` status bit no more than once per second will ensure that interrupts are not generated at too fast a rate.

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

SKW115. Removed

SKW116. Core and/or Ring Frequency May Be Briefly Lower Than Expected After BIOS Completes

Problem: Due to this erratum, the core and ring frequencies may be lower than expected for up to several seconds after BIOS completes

Implication: Processing immediately after BIOS completes may take longer than expected. The erratum does not cause any functional failures.

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.

SKW117. Resume Flag (RF) May be Incorrectly Set in The EFLAGS That Is Saved on a Fault in PEBS or BTS

Problem: After a fault due to a failed PEBS or BTS address translation, the RF may be incorrectly set in the EFLAGS image that is saved.

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

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

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

SKW118. Some Memory Performance Monitoring Events May Produce Incorrect Results When Filtering on Either OS or USR Modes

Problem: The memory at-retirement performance monitoring events (next listed) may produce incorrect results when a performance counter is configured in OS-only or USR-only modes (bits 17 or 16 in `IA32_PERFEVTSELx` MSR). Counters with both OS and USR bits set are not affected by this erratum.

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

```
MEM_INST_RETIRED.STLB_MISS_LOADS event D0H, umask 11H
MEM_INST_RETIRED.STLB_MISS_STORES event D0H, umask 12H
MEM_INST_RETIRED.LOCK_LOADS event D0H, umask 21H
MEM_INST_RETIRED.SPLIT_LOADS event D0H, umask 41H
MEM_INST_RETIRED.SPLIT_STORES event D0H, umask 42H
MEM_LOAD_RETIRED.L2_HIT event D1H, umask 02H
MEM_LOAD_RETIRED.L3_HIT event D1H, umask 04H
MEM_LOAD_RETIRED.L4_HIT event D1H, umask 80H
MEM_LOAD_RETIRED.L1_MISS event D1H, umask 08H
MEM_LOAD_RETIRED.L2_MISS event D1H, umask 10H
MEM_LOAD_RETIRED.L3_MISS event D1H, umask 20H
MEM_LOAD_RETIRED.FB_HIT event D1H, umask 40H
MEM_LOAD_L3_HIT_RETIRED.XSNP_MISS event D2H, umask 01H
MEM_LOAD_L3_HIT_RETIRED.XSNP_HIT event D2H, umask 02H
MEM_LOAD_L3_HIT_RETIRED.XSNP_HITM event D2H, umask 04H
MEM_LOAD_L3_HIT_RETIRED.XSNP_NONE event D2H, umask 08H
```

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

Workaround: None identified.

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

SKW119. RING_PERF_LIMIT_REASONS May be Incorrect

Problem: Under certain conditions, `RING_PERF_LIMIT_REASONS` (MSR 6B1H) may incorrectly assert the OTHER status bit (bit 8) as well as the OTHER log bit [bit 24].

Implication: When this erratum occurs, software using this register will incorrectly report clipping because of the OTHER reason.

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.

SKW120. The HWP May Generate Thermal Interrupt While Not Enabled

Problem: Due to this erratum, the conditions for HWP to generate a thermal interrupt on a logical processor may generate thermal interrupts on both logical processors of that core.

Implication: If two logical processors of a core have different configurations of the HWP (for example, only enabled on one), an unexpected thermal interrupt may occur on one logical processor due to the HWP settings of the other logical processor.

Workaround: Software should configure the HWP consistently on all logical processors of a core.

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

SKW121. Camera Device Does Not Issue an Message Signaled Interrupts (MSI) When INTx is Enabled

Problem: When both MSI and legacy INTx are enabled by the camera device, INTx is asserted rather than issuing the MSI, in violation of the PCI Local Bus Specification.

Implication: Due to this erratum, camera device interrupts can be lost leading to device failure.

Workaround: The camera device must disable legacy INTx by setting bit 10 of PCICMD (Bus 0; Device 5; Function 0; Offset 04H) before MSI is enabled

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

SKW122. Violations of Intel® SGX Access-Control Requirements Produce #GP Instead of Page Fault (#PF)

Problem: Intel® SGX define new access-control requirements on memory accesses. A violation of any of these requirements causes a #PF that sets bit 15 (Intel® SGX) in the page-fault error code. Due to this erratum, these violations instead cause general-protection exceptions (#GP).

Implication: Software resuming from system sleep states S3 or S4 and relying on receiving a page fault from the previous enclave accesses may not operate properly.

Workaround: Software can monitor #GP faults to detect that an enclave has been destroyed and needs to be rebuilt after resuming from S3 or S4.

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

SKW123. PCIe* Graphics (PEG) Advanced Error Reporting (AER) is Not Enabled

Problem: The PCIe* and PEG AER capability is not enabled for Server/Workstation SKUs.

Implication: Software cannot use AER capabilities.

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.

SKW124. Performance Monitoring Counters May Undercount When Using CPL Filtering

Problem: Performance Monitoring counters configured to count only OS or only USR events by setting exactly one of bits 16 or 17 in `IA32_PERFEVTSELx` MSRs (186H-18DH) may not count for a brief period during the transition to a new CPL.

Implication: A measurement of ring transitions (using the edge-detect bit 18 in `IA32_PERFEVTSELx`) may undercount, such as `CPL_CYCLES.RING0_TRANS` (Event 5CH, Umask 01H). Additionally, the sum of an OS-only event and a USR-only event may not exactly equal an event counting both OS and USR. Intel has not observed any other software-visible impact.

Workaround: None identified.

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

SKW125. SMRAM State-Save Area Above the 4 GB Boundary May Cause Unpredictable System Behavior

Problem: If the BIOS uses the RSM instruction to load the SMBASE register with a value that would cause any part of the SMRAM state-save area to have an address above 4 GBytes, subsequent transitions into and out of SMM might save and restore processor state from incorrect addresses.

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

Workaround: Ensure that the SMRAM state-save area is located entirely below the 4 GB address boundary.

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

SKW126. Certain Non-Canonical IA32_BNDCFGS Values Will Not Cause VM-Entry Failures

Problem: If the VM-entry controls Load IA32_BNDCFGS field (bit 16) is 1, VM-entry should fail when the value of the guest IA32_BNDCFGS field in the VMCS is not canonical (that is, when bits 63:47 are not identical). Due to this erratum, VM-entry does not fail if bits 63:48 are identical but differ from bit 47. In this case, VM-entry loads the IA32_BNDCFGS MSR with a value in which bits 63:48 are identical to the value of bit 47 in the VMCS field.

Implication: If the value of the guest IA32_BNDCFGS field in the VMCS is not canonical, VM-entry may load the IA32_BNDCFGS MSR with a value different from that of the VMCS field.

Workaround: None identified.

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

SKW127. PEBS EventingIP Field May Be Incorrect Under Certain Conditions

Problem: The EventingIP field in the PEBS record reports the address of the instruction that triggered the PEBS event. Under certain complex microarchitectural conditions, the EventingIP field may be incorrect.

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

Workaround: None identified.

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

SKW128. Executing a 256 Bit Intel® AVX Instruction May Cause Unpredictable Behavior

Problem: Under complex microarchitectural conditions, executing a 256 Intel® AVX bit instruction may result in unpredictable system behavior.

Implication: When this erratum occurs, the system may behave unpredictably.

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.

SKW129. An x87 Store Instruction Which Pends Precision Exception (#PE) May Lead to Unexpected Behavior When EPT A/D Is Enabled.

Problem: An x87 store instruction which causes a #PE to be pended and updates an EPT A/D bit and causes a VM exit (such as EPT violation or #PF VM exit) may lead to unexpected behavior.

Implication: The VMM may experience unexpected x87 fault or a machine check exception with the value of 0x150 in `IA32_MC0_STATUS.MCACOD` (bits [15:0] in MSR 401H).

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.

SKW130. PECI May Not Be Functional After Power On or S3/S4/S5 Resume

Problem: When resuming from S3/S4/S5 or following a power on, PECI may fail to function properly.

Implication: When this erratum occurs, the PECI does not respond to any 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.

SKW131. A System Hang or Machine Check May Occur When eDRAM Is Enabled

Problem: When eDRAM is enabled, the processor may experience a hang or a machine check exception with an error reported in `IA32_MC10_STATUS`.

Implication: When this erratum occurs, the system will generate a machine check error or 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.

SKW132. Load Latency Performance Monitoring Facility May Stop Counting

Problem: The performance monitoring events `MEM_TRANS_RETIRED.LOAD_LATENCY_*` (Event CDH; UMask 01H; any latency) count load instructions whose latency exceed a predefined threshold, where the loads are randomly selected using the Load Latency facility (PEBS extension). However, due to this erratum, load latency facility may stop counting load instructions when Intel® Hyper-Threading Technology (Intel® HT Technology) is enabled.

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

Workaround: None identified.

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

SKW133. BNDLDX And BNDSTX May Not Signal #GP on Non-Canonical Bound Directory Access

Problem: BNDLDX and BNDSTX instructions access the bound’s directory and table to load or store bounds. These accesses should signal #GP when the address is not canonical (for example, bits 48 to 63 are not the sign extension of bit 47). Due to this erratum, #GP may not be generated by the processor when a non-canonical address is used by BNDLDX or BNDSTX for their bound directory memory access.

Implication: Intel has not observed this erratum with any commercially available software.

Workaround: Software should use canonical addresses for bound directory accesses.

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

SKW134. Digital Thermal Sensor (DTS) Temperature Reading May Be Inaccurate on DDR4 systems

Problem: The temperature reported by the DTS on DDr4 systems may vary from the actual temperature by +5 °C to -15 °C rather than the specified ±5 °C.

Implication: When this erratum occurs, CPU throttling may occur later than expected. Intel has not observed this erratum to have any impact on system.

Workaround: None identified.

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

SKW135. Performance Monitoring Load Latency Events May Be Inaccurate For Gather Instructions

Problem: The performance monitoring events `MEM_TRANS_RETIRED.LOAD_LATENCY_*` (Event CDH; UMask 01H; any latency) count load instructions whose latency exceed a predefined threshold, where the loads are randomly selected using the load latency facility (an extension of PEBS). However, due to this erratum, these events may count incorrectly for VGATHER/VPGATHER instructions.

Implication: The Load Latency Performance Monitoring events may be inaccurate for Gather instructions.

Workaround: None identified.

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

SKW136. IA32_RTIT_CR3_MATCH MSR Bits[11:5] Are Treated As Reserved

Problem: Due to this erratum, bits [11:5] in `IA32_RTIT_CR3_MATCH` (MSR 572H) are reserved; an MSR write that attempts to set that field to a non-zero value will result in a #GP fault.

Implication: The inability to write the identified bit field does not affect the functioning of Intel® PT operation because, as described in erratum SKL061, the bit field that is the subject of this erratum is not used during Intel® PT CR3 filtering.

Workaround: Ensure that bits 11:5 of the value written to `IA32_RTIT_CR3_MATCH` are zero, including cases where the selected page-directory-pointer-table base address has non-zero bits in this range.

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

SKW137. APIC Timer Interrupt May Not Be Generated at The Correct Time In TSC-Deadline Mode

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

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

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

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

SKW138. Some Bits in MSR_MISC_PWR_MGMT May Be Updated on Writing Illegal Values to This MSR

Problem: Attempts to write illegal values to `MSR_MISC_PWR_MGMT` (MSR 0x1AA) result in #GP and should not change the MSR value. Due to this erratum, some bits in the MSR may be updated on writing an illegal value.

Implication: Certain fields may be updated with allowed values when writing illegal values to `MSR_MISC_PWR_MGMT`. Such writes will always result in #GP as expected.

Workaround: None identified. Software should not attempt to write illegal values to this MSR.

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

SKW139. Unpredictable System Behavior May Occur When System Agent Enhanced Intel® SpeedStep Technology Is Enabled

Problem: Under complex system conditions, system agent enhanced Intel® SpeedStep Technology may result in unpredictable system behavior.

Implication: When this erratum occurs, the system may behave unpredictably.

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.

SKW140. Processor May Hang Under Complex Scenarios

Problem: Under complex microarchitectural conditions, the processor may hang with an internal timeout error (MCACOD 0400H) logged into `IA32_MCi_STATUS`.

Implication: This erratum results in a processor 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.

SKW141. The Intel® PT CR3 Filter Is Not Re-evaluated on VM Entry

Problem: On a VMRESUME or VMLAUNCH with both TraceEn[0] and CR3Filter[7] in `IA32_RTIT_CTL` (MSR 0570H) set to 1 both before the VM Entry and after, the new value of CR3 is not compared with `IA32_RTIT_CR3_MATCH` (MSR 0572H).

Implication: The Intel® PT CR3 filtering mechanism may continue to generate packets despite a mismatching CR3 value, or may fail to generate packets despite a matching CR3, as a result of an incorrect value of `IA32_RTIT_STATUS`.ContextEn[1] (MSR 0571H) that results from the failure to re-evaluate the CR3 match on VM entry.

Workaround: None identified.

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

SKW142. Display Slowness May Be Observed Under Certain Display Commands Scenario

Problem: Back-to-back accesses to the VGA register ports (I/O addresses 0x3C2, 0x3CE, 0x3CF) will experience higher than expected latency.

Implication: Due to this erratum, the processor may redraw the screen slowly when in VGA mode.

Workaround: None identified.

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

SKW143. CPUID TLB Associativity Information Is Inaccurate

Problem: CPUID leaf 2 (EAX=02H) TLB information inaccurately reports that the shared second-level TLB is 6-way set associative (value C3H), although it is 12-way set associative. Other information reported by CPUID leaf 2 is accurate.

Implication: Software that uses CPUID shared second-level TLB associativity information for value C3H may operate incorrectly. Intel has not observed this erratum to impact the operation of any commercially available software.

Workaround: None identified. Software should ignore the shared second-level TLB associativity information reported by CPUID for the affected processors.

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

SKW144. Short Loops Which Use AH/BH/CH/DH Registers May Cause Unpredictable System Behavior

Problem: Under complex microarchitectural conditions, short loops of less than 64 instructions that use AH, BH, CH or DH registers as well as their corresponding wider register (for example, RAX, EAX or AX for AH) may cause unpredictable system behavior. This can only happen when both logical processors on the same physical processor are active.

Implication: Due to this erratum, the system may experience 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.

SKW145. Processor Graphics May Render Incorrectly or May Hang Following Warm Reset With Package C8 Disabled

Problem: Processor Graphics may not properly restore internal configuration after warm reset when package C8 is disabled.

Implication: Due to this erratum Processor Graphics may render incorrectly or hang on warm reset.

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.

SKW146. Unpredictable System Behavior May Occur in DDR4 Multi-Rank System

Problem: Due to incorrect configuration of DDR4 ODT by BIOS, it is possible for a multi-rank system to violate Section 4.27 of the DDR4 JEDEC specification revision JESED79-4A.

Implication: Due to this erratum, complex microarchitectural conditions may result in unpredictable system behavior.

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

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

SKW147. Processor May Hang on Complex Sequence of Conditions

Problem: A complex set of architectural and microarchitectural conditions may lead to a processor hang with an internal timeout error (MCACOD 0400H) logged into `IA32_MC3_STATUS` (MSR 040DH, bits [15:0]). When both logical processors in a core are active, this erratum will not occur in one logical processor unless there is no interrupt for more than 10 seconds to the other logical processor.

Implication: This erratum may result in a processor hang. 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.

SKW148. Display Artifacts May Be Seen With High Bandwidth, Multiple Display Configurations

Problem: With high bandwidth, multiple display configurations, display engine underruns may occur.

Implication: Due to this erratum, the display engine may generate display artifacts.

Workaround: This erratum can be worked around by Graphics Driver revisions of 15.46.4.64.4749 or later.

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

SKW149. Spurious Corrected Errors May Be Reported

Problem: Due to this erratum, spurious corrected errors may be logged in the `IA32_MC0_STATUS` MSR (401H) register with the valid field [bit 63] set, the uncorrected error field bit [bit 61] not set, a model specific error code (bits [31:16]) of 0x0001, and an MCA error code (bits [15:0]) of 0x0005. If CMCI is enabled, these spurious corrected errors also signal interrupts.

Implication: When this erratum occurs, software may see an unusually high rate of reported corrected errors. As it is not possible to distinguish between spurious and non-spurious errors, this erratum may interfere with reporting non-spurious corrected errors.

Workaround: None identified.

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

SKW150. Masked Bytes in a Vector Masked Store Instructions May Cause Write Back of a Cache Line

Problem: Vector masked store instructions to the WB memory-type that cross cache lines may lead to a CPU writing back cached data even for cache lines where all of the bytes are masked.

Implication: The processor may generate writes of unmodified data. This can affect MMIO or non-coherent agents in the following ways:

1. For MMIO range that is mapped as WB memory type, this erratum may lead to Machine Check Exception (MCE) due to writing back data into the MMIO space. This applies only to cross page vector masked stores where one of the pages is in MMIO range.

2. If the CPU cached data is stale, for example in the case of memory written directly by a non-coherent agent (agent that uses non-coherent writes), this erratum may lead to writing back stale cached data even if these bytes are masked.

Workaround: Platforms should not map MMIO memory space or non-coherent device memory space as a WB memory. If a WB is used for the MMIO range, software or VMM should not map such MMIO page adjacent to a regular WB page (adjacent on the linear address space, before or after the I/O page). Memory that may be written by non-coherent agents should be separated by at least 64 bytes from regular memory used for other purposes (on the linear address space).

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

SKW151. Processor May Incorrectly Assert PROCHOT During PkgC10

Problem: If the PROCHOT# pin is configured as an output-only signal, PROCHOT# may incorrectly be asserted during PkgC10.

Implication: When this erratum occurs, PROCHOT# may be incorrectly asserted. This can lead to the system fan unnecessarily turning on during PkgC10 or other unexpected platform behaviors.

Workaround: None identified.

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

SKW152. Writing Non-Zero Values to Read Only Fields in IA32_THERM_STATUS MSR May #GP

Problem: `IA32_THERM_STATUS` MSR (19CH) includes Read-Only (RO) fields as well as writable fields. Writing a non-zero value to any of the read-only fields may cause a #GP.

Implication: Due to this erratum, software that reads the `IA32_THERM_STATUS` MSR, modifies some of the writable fields, and attempts to write the MSR back may #GP.

Workaround: Software should clear all read-only fields before writing to this MSR

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

SKW153. Precise Performance Monitoring May Generate Redundant PEBS Records

Problem: PEBS may generate redundant records for a counter overflow when used to profile cycles. This may occur when a precise performance monitoring event is configured on a general counter while setting the Invert and Counter Mask fields in `IA32_PERFEVTSELx` MSRs (186H - 18DH), and the counter is reloaded with a value smaller than 1000 (through the PEBS-counter-reset field of the DS Buffer Management Area).

Implication: PEBS may generate multiple redundant records when used to profile cycles in certain conditions.

Workaround: It is recommended for software to forbid the use of the Invert bit in `IA32_PERFEVTSELx` MSRs or restrict PEBS-counter-reset value to a value of at least 1000.

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

SKW154. Intel® SGX ENCLS[EINIT] May Not Signal an Error For an Incorrectly Formatted SIGSTRUCT Input

Problem: The ENCLS[EINIT] instruction leaf may not signal an error on a specific combination of SIGSTRUCT values even though the signature does not fully comply with the RSA signature specifications.

Implication: When this erratum occurs, the ENCLS[EINIT] instruction leaf may pass the checks although the SIGSTUCT signature does not fully comply with the RSA signature specifications. This erratum does not compromise the security of Intel® SGX and does not impact normal usage of Intel® SGX.

Workaround: None identified. Software is not expected to be impacted by this erratum.

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

SKW155. Branch Instruction Address May Be Incorrectly Reported on Intel® TSX Abort When Using Intel® MPX

Problem: When using Intel® MPX, an Intel® TSX transaction abort will occur in case of legacy branch (that causes bounds registers INIT) when at least one Intel® MPX bounds register was in a NON-INIT state. On such an abort, the branch Instruction address should be reported in the `FROM_IP` field in the Last Branch Record (LBR), the BTS and BTM as well as in the FUP source IP address for Intel® PT. Due to this erratum, the `FROM_IP` field in LBR/BTS/BTM, as well as the FUP source IP address that correspond to the Intel® TSX abort, may point to the preceding instruction.

Implication: Software that relies on the accuracy of the FROM_IP field/FUP source IP address and uses Intel® TSX may operate incorrectly when Intel® MPX is used.

Workaround: None identified.

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

SKW156. Setting Performance Monitoring IA32_PERF_GLOBAL_STATUS_SET MSR Bit 63 May Not #GP

Problem: Bit 63 of `IA32_PERF_GLOBAL_STATUS_SET` MSR (391H) is reserved. Due to this erratum, setting the bit will not result in a #GP.

Implication: Software that attempts to set bit 63 of `IA32_PERF_GLOBAL_STATUS_SET` MSR does not generate #GP. There are no other system implications to this behavior.

Workaround: None identified.

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

SKW157. Hitting a Code Breakpoint Inside a Intel® SGX Debug Enclave May Cause The Processor to Hang

Problem: Under complex microarchitecture conditions, the processor may hang when hitting code breakpoint inside a Intel® SGX debug enclave. This may happen only after opt-out entry into a Intel® SGX debug enclave and when the execution would set the accessed bit (A-bit) in any level of the paging or EPT structures used to map the code page, and when both logical processors on the same physical core are active.

Implication: Due to this erratum, the processor may hang while debugging an Intel® SGX debug enclave.

Workaround: None identified.

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

SKW158. Performance Monitoring Anti Side-Channel Interference (ASCI) Status Bit May be Inaccurate

Problem: The ASCI field in IA32_PERF_GLOBAL_STATUS (MSR 38EH, bit 60) should be set when the count in any of the configured performance counters (for example, IA32_PMCx or IA32_FIXED_CTRx) was altered due to direct or indirect operation of Intel® SGX. Due to this erratum, the ASCI bit may not be set properly when IA32_FIXED_CTR0 is used.

Implication: Software that relies on the value of the ASCI bit in IA32_PERF_GLOBAL_STATUS for its operation may not operate correctly when IA32_FIXED_CTR0 is used.

Workaround: None identified.

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

SKW159. Processor May Hang When Executing Code In an Hardware Lock Elision (HLE) Transaction Region

Problem: Under certain conditions, if the processor acquires an HLE lock via the XACQUIRE instruction in the Host Physical Address range between 40000000H and 403FFFFFH, it may hang with an internal timeout error (MCACOD 0400H) logged into IA32_MCi_STATUS.

Implication: Due to this erratum, the processor may hang after acquiring a lock via XACQUIRE.

Workaround: The BIOS can reserve the host physical address ranges of 40000000H and 403FFFFFH (for example, map it as UC/MMIO). Alternatively, VMM can reserve that address range so no guest can use it. In non-virtualized systems, the OS can reserve that memory space.

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

SKW160. Intel® PT CYC Packet Can Be Dropped When Immediately Preceding PSB

Problem: Due to a rare microarchitectural condition, generation of an Intel® PT PSB packet can cause a single Cycle Count (CYC) packet, possibly along with an associated MTC packet, to be dropped.

Implication: An Intel® PT decoder that is using CYCs to track time or frequency will get an improper value due to the lost CYC packet.

Workaround: If an Intel® PT decoder is using CYCs and MTCs to track frequency, and either the first MTC following a PSB shows that an MTC was dropped, or the CYC value appears to be 4095 cycles short of what is expected, the CYC value associated with that MTC should not be used. The decoder should wait for the next MTC before measuring frequency again.

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

SKW161. Intel® PT VM-entry Indication Depends on The Incorrect VMCS Control Field

Problem: An Intel® PT Paging Information Packet (PIP), which includes indication of entry into non-root operation, will be generated on VM-entry as long as the “Conceal VMX in Intel® PT” field [Bit 19] in Secondary Execution Control register (`IA32_VMX_PROCBASED_CTLS2`, MSR 048BH) is clear. This diverges from expected behavior, since this PIP should instead be generated only with a zero value of the “Conceal VMX entries from Intel® PT” field [Bit 17] in the Entry Control register (`IA32_VMX_ENTRY_CTLS` MSR 0484H).

Implication: An Intel® PT trace may incorrectly expose entry to non-root operation.

Workaround: A VMM should always set both the “Conceal VMX entries from Intel® PT” field in the Entry Control register and the “Conceal VMX in Intel® PT” in the Secondary Execution Control register to the same value.

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

SKW162. VCVTPS2PH To Memory May Update MXCSR in The Case of a Fault on the Store

Problem: Execution of the VCVTPS2PH instruction with a memory destination may update the MXCSR exceptions flags (bits [5:0]) if the store to memory causes a fault (for example, #PF) or VM exit. The value written to the MXCSR exceptions flags is what would have been written if there were no fault.

Implication: Software may see exceptions flags set in MXCSR, although the instruction has not successfully completed due to a fault on the memory operation. Intel has not observed this erratum to affect any commercially available software.

Workaround: None identified.

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

SKW163. Intel® PT May Drop All Packets After an Internal Buffer Overflow

Problem: Due to a rare microarchitectural condition, an Intel® PT Table of Physical Addresses (ToPA) entry transition can cause an internal buffer overflow that may result in all trace packets, including the OVF packet, being dropped.

Implication: When this erratum occurs, all trace data will be lost until either Intel® PT is disabled and re-enabled via `IA32_RTIT_CTL`.TraceEn [bit 0] (MSR 0570H) or the processor enters and exits a C6 or deeper C state.

Workaround: None identified.

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

SKW164. ZMM/YMM Registers May Contain Incorrect Values

Problem: Under complex microarchitectural conditions, values stored in ZMM and YMM registers may be incorrect.

Implication: Due to this erratum, YMM and ZMM registers may contain an incorrect value. 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 Tables of Changes.

SKW165. Intel® PT ToPA Tables Read From Non-Cacheable Memory During an Intel® TSX Transaction May Lead to Processor Hang

Problem: If an Intel® PT ToPA table is placed in Uncacheable (UC) or Uncacheable Speculative Write Combining (USWC) memory, and a ToPA output region is filled during an Intel® TSX transaction, the resulting ToPA table read may cause a processor hang.

Implication: Placing Intel® PT ToPA tables in non-cacheable memory when Intel® TSX is in use may lead to a processor hang.

Workaround: None identified. Intel® PT ToPA tables should be located in WB memory if Intel® TSX is in use.

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

SKW166. Performing an XACQUIRE to an Intel® PT ToPA Table May Lead to Processor Hang

Problem: If an XACQUIRE lock is performed to the address of an Intel® PT ToPA table, and that table is later read by the CPU during the HLE transaction, the processor may hang.

Implication: Accessing ToPA tables with XACQUIRE may result in a processor hang.

Workaround: None identified. Software should not access ToPA tables using XACQUIRE. An OS or hypervisor may wish to ensure all application or guest writes to ToPA tables to take page faults or EPT violations.

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

SKW167. When Virtualization Exceptions are Enabled, EPT Violations May Generate Erroneous Virtualization Exceptions

Problem: An access to a Guest-Physical Address (GPA) may cause an EPT-violation VM exit. When the “EPT-violation Virtualization Exception (#VE)” VM-execution control is 1, an EPT violation may cause a #VE instead of a VM exit. Due to this erratum, an EPT violation may erroneously cause a #VE when the “suppress #VE” bit is set in the EPT paging-structure entry used to map the GPA being accessed. This erratum does not apply when the “EPT-violation #VE” VM-execution control is 0 or when delivering an event through the IDT. This erratum applies only when the GPA in CR3 is used to access the root of the guest paging-structure hierarchy (or, with PAE paging, when the GPA in a PDPTE is used to access a page directory).

Implication: When using PAE paging mode, an EPT violation that should cause an VMexit in the VMM may instead cause a VE# in the guest. In other paging modes, in addition to delivery of the erroneous #VE, the #VE may itself cause an EPT violation, but this EPT violation will be correctly delivered to the VMM.

Workaround: A VMM may support an interface that guest software can invoke with the VMCALL instruction when it detects an erroneous #VE.

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

SKW168. Using Intel® TSX Instructions May Lead to Unpredictable System Behavior

Problem: Under complex microarchitectural conditions, software using Intel® TSX may result in unpredictable system behavior. Intel has only seen this under synthetic testing conditions. Intel is not aware of any commercially available software exhibiting this behavior.

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

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

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

SKW169. Performance Monitoring General Purpose Counter 3 May Contain Unexpected Values

Problem: When the RTM is supported (CPUID.07H.EBX.RTM [bit 11] = 1) and when `TSX_FORCE_ABORT=0`, Performance Monitor Unit (PMU) general purpose counter 3 (`IA32_PMC3`, MSR C4H and IA32_A_PMC3, MSR 4C4H) may contain unexpected values. Further, `IA32_PREFEVTSEL3` (MSR 189H) may also contain unexpected configuration values.

Implication: Due to this erratum, software that uses PMU general purposes counter 3 may read an unexpected count and configuration.

Workaround: Software can avoid this erratum by writing 1 to bit 0 of `TSX_FORCE_ABORT` (MSR 10FH), which will cause all Restricted Transactional Memory (RTM) transactions to abort with EAX code 0. `TSX_FORCE_ABORT` MSR is available when CPUID.07H.EDX[bit 13]=1

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

SKW170. Intel® PT Trace May Silently Drop Second Byte of CYC Packet

Problem: Due to a rare microarchitectural condition, the second byte of a 2-byte CYC packet may be dropped without an OVF packet.

Implication: A trace decoder may signal a decode error due to the lost trace byte.

Workaround: None identified. A mitigation is available for this erratum. If a decoder encounters a multi-byte CYC packet where the second byte has bit 0 (Ext) set to 1, it should assume that 4095 cycles have passed since the prior CYC packet, and it should ignore the first byte of the CYC and treat the second byte as the start of a new packet.

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

SKW171. Unexpected Uncorrected Machine Check Errors May Be Reported

Problem: In rare microarchitectural conditions, the processor may report unexpected machine check errors. When this erratum occurs, `IA32_MC0_STATUS` (MSR 401H) will have the valid bit set [bit 63], the uncorrected error bit set [bit 61], a model specific error code of 03H (bits [31:16]) and an MCA error code of 05H (bits [15:0]).

Implication: Due to this erratum, software may observe unexpected machine check exceptions.

Workaround: None identified.

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

SKW172. Gen9 Graphics VT-d Hardware May Cache Invalid Entries

Problem: The Gen9 graphics subsystem may cache invalid Intel® VT-d context entries.

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

Workaround: Software should flush the Gfx Intel® VT-d context cache after any update of context table entries.

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

SKW173. A Pending Fixed Interrupt May Be Dispatched Before an Interrupt of The Same Priority Completes

Problem: Resuming from C6 Sleep-State, with Fixed Interrupts of the same priority queued (in the corresponding bits of the Intel Reuse Repository [IRR] and Intel Strategic Research [ISR] APIC registers), the processor may dispatch the second interrupt (from the IRR bit) before the first interrupt has been completed and written to the End-of-Interrupt (EOI) register, causing the first interrupt to never complete.

Implication: Due to this erratum, software may behave unexpectedly when an earlier call to an Interrupt Handler routine is overridden with another call (to the same Interrupt Handler) instead of completing its execution.

Workaround: None idntified.

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

SKW174. Executing Some Instructions May Cause Unpredictable Behavior

Problem: Under complex microarchitectural conditions, executing an X87, Intel® AVX, or integer divide instruction may result in unpredictable system behavior.

Implication: When this erratum occurs, the system may behave unpredictably. 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 Tables of Changes.

SKW175. Incorrect Execution of Internal Branch Instructions May Lead to Unpredictable System Behavior

Problem: Under complex microarchitecture conditions, incorrect execution of internal branch instructions that span multiple 64-byte boundaries (cross cache line), may result in unpredictable system behavior including unexpected #PF or #UD faults due to incorrect execution of internal branch operations.

Implication: When this erratum occurs, the system may exhibit unpredictable system behavior including unexpected #PF or #UD faults.

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.

SKW176. Unexpected Page Faults in Guest Virtualization Environment

Problem: Under complex microarchitectural conditions, a virtualized guest could observe unpredictable system behavior.

Implication: When this erratum occurs, systems operating in a virtualization environment may exhibit unexpected page faults (double faults) leading to guest OS shutdown.

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.

SKW177. Intel® SGX Key Confidentiality May Be Compromised

Problem: Under complex microarchitectural conditions, it may be possible for the value of Intel® SGX keys to be inferred using speculative execution side channel methods.

Implication: If exposed, such keys could allow an attacker to access Intel® SGX enclave data. Processors that do not support Intel® HT Technology are not affected by this issue.

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.

SKW178. Instruction Fetch May Cause Machine Check if Page Size Was Changed Without Invalidation

Problem: This erratum may cause a machine-check error (IA32_MCi_STATUS.MCACOD=005H with IA32_MCi_STATUS.MSCOD=00FH or IA32_MCi_STATUS.MCACOD=0150H with IA32_MCi_STATUS.MSCOD=00FH) on the fetch of an instruction. It applies only if (1) instruction bytes are fetched from a linear address translated using a 4-Kbyte page and cached in the processor; (2) the paging structures are later modified so that these bytes are translated using a large page (2 Mbyte, 4 Mbyte or 1 GB) with a different Physical Address (PA), memory type (PWT, PCD and PAT bits), or User/Supervisor (U/S) bit; and (3) the same instruction is fetched after the paging structure modification but before software invalidates any TLB entries for the linear region.

Problem: Implication: Due to this erratum an unexpected machine check with error code 0150H with MSCOD 00FH may occur, possibly resulting in a shutdown. This erratum could also lead to unexpected correctable machine check (IA32_MCi_STATUS.UC=0) with error code 005H with MSCOD 00FH

Implication: Due to this erratum an unexpected machine check with error code 0150H with MSCOD 00FH may occur, possibly resulting in a shutdown. This erratum could also lead to unexpected correctable machine check (IA32_MCi_STATUS.UC=0) with error code 005H with MSCOD 00FH.

Workaround: Software should not write to a paging-structure entry in a way that would change the page size and either the physical address, memory type or User/Supervisor bit. It can instead use one of the following algorithms: first, clear the P flag in the relevant paging-structure entry (for example, PDE); then, invalidate any translations for the affected linear addresses; and then, modify the relevant paging-structure entry to set the P flag and establish the new page size. An alternative algorithm: first, change the physical page attributes (combination of physical address, memory type and User/Supervisor bit) in all 4K pages in the affected linear addresses; then, invalidate any translations for the affected linear addresses; and the,n modify the relevant paging-structure entry to establish the new page size.

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

SKW179. System May Hang Under Complex Conditions

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

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

Workaround: It is possible for a combination of BIOS and a graphics driver to contain a workaround for this erratum.

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

SKW180. PEG PCIe* Link May Fail to Link When Resuming From PKG-C8

Problem: The PEG IO registers may not be restored after resuming from PKG-C8.

Implication: PEG PCIe* may fail to link resuming from PKG-C8.

Workaround: None identified.

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

SKW181. Incorrect Error Correcting Code (ECC) Reporting Following Entry to PKG-C7

Problem: Correctable and Uncorrectable ECC errors reported in ECCERRLOG0/1 (MCHBAR Offset 4048h/404Ch) may be overwritten after entry to PKG-C7.

Implication: DDR4 Correctable and Uncorrectable ECC errors reported in ECCERRLOG0/1 (MCHBAR Offset 4048h/404Ch) may be unreported resuming from PKG-C7. Intel has only observed this erratum in a synthetic test environment.

Workaround: None identified.

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

SKW182. PMU MSR_UNC_PERF_FIXED_CTR Is Cleared After Pkg C7 or Deeper

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

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

Workaround: None identified.

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

SKW183. Performance Monitoring General Counter 2 May Have Invalid Value Written When Intel® TSX Is Enabled

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

Implication: Software may read invalid value from `IA32_PMC2`.

Workaround: None identified

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

SKW184. Overflow Flag in IA32_MC0_STATUS MSR May Be Incorrectly Set

Problem: Under complex microarchitectural conditions, a single internal parity error seen in `IA32_MC0_STATUS` MSR (401h) with MCACOD (bits 15:0) value of 5h and MSCOD (bits 31:16) value of 7h, may set the overflow flag (bit 62) in the same MSR.

Implication: Due to this erratum, the `IA32_MC0_STATUS` overflow flag may be set after a single parity error. Intel has not observed this erratum with any commercially available software.

Workaround: None identified.

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

SKW185. VERR Instruction Inside VM-entry May Cause DR6 to Contain Incorrect Values

Problem: Under complex microarchitectural conditions, a VERR instruction that follows a VM-entry with a guest state indicating MOV SS blocking (bit 1 in the Interruptibility state) and at least one of B3-B0 bits set (bits 3:0 in the pending debug exception), may lead to incorrect values in DR6.

Implication: Due to this erratum, DR6 may contain incorrect values. Intel has not observed this erratum with any commercially available software.

Workaround: None identified.

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

SKW186. Processor May Hang If Warm Reset Triggers While BIOS Is Initialization

Problem: Under complex microarchitectural conditions, when the processor receives a warm reset during the BIOS initialization, the processor may hang with a machine check error reported in IA32_MCi_STATUS, with MCACOD (bits [15:0]) value of 0400H, and MSCOD (bits [31:16]) value of 0080H.

Implication: Due to this erratum, the processor may hang. Intel has only observed this erratum in a synthetic test environment.

Workaround: None identified.

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

SKW187. A PMI That Freezes LBRs Can Cause a Duplicate Entry in TOS

Problem: If a PMI is taken while the LBRs are enabled and IA32_DEBUGCTL.FREEZE_LBRS_ON_PMI[bit11]=1 (MSR 01D9H), a taken branch that performs an LBR update near the time of the PMI may instead record a duplicate of the prior entry into the Top of Stack (ToS) entry.

Implication: Software may unexpectedly observe the appearance of back-to-back execution of the same branch.

Workaround: In general, software can ignore the ToS entry if it matches the ToS-1 entry. Note that certain code sequences with no intervening taken branches can legitimately insert a valid duplicate LBR record in the ToS entry.

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

SKW188. Display Intel® VT-d TLB Invalidation during Disabling of Intel® VT-d Translations May Cause Display Corruption or Flickering

Problem: If a hypervisor or VMM has enabled Intel® VT-d translations for the Gfx IOMMU (TE=1 in Intel® VT-d specification) and then switches the Gfx IOMMU to disable translations (TE=0) with DMA remapping enabled in the BIOS, the display Intel® VT-d TLB may be invalidated without waiting for any pending memory requests to complete.

Implication: Due to this erratum, momentary display corruption or flickering may occur during boot.

Workaround: None identified.

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

SKW189. MD_CLEAR Operations May Not Properly Overwrite All Buffers

Problem: On processors that enumerate the MD_CLEAR CPUID bit (CPUID.(EAX=7H,ECX=0):EDX[MD_CLEAR=10]), L1D_FLUSH, RSM and VERW memory instructions should overwrite affected buffers with constant data. Under complex microarchitectural conditions, these instructions may not overwrite all affected buffers.

Implication: Due to this erratum, the use of MD_CLEAR operations to prevent Microarchitectural Data Sampling (MDS) or Intel® Transactional Synchronization Extensions (Intel® TSX) Asynchronous Abort side-channel methods from revealing previously accessed data may not be fully effective.

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.

SKW190. Unexpected Code Breakpoint May Occur

Problem: An unexpected code breakpoint may occur in one logical thread on a physical core while another logical thread on the same physical core is performing a Branch Prediction Unit Flush (MSR 0x49, bit [0] set to 1).

Implication: Due to this erratum, the processor may take an unexpected code breakpoint exception. Software that is not configured to manage such an exception may not operate as expected.

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

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

SKW191. Incorrect MCACOD for L2 MCE

Problem: Under complex microarchitectural conditions, an L2 poison MCE that should be reported with MCACOD 189h in IA32_MC3_STATUS MSR (MSR 40dh, bits [15:0]) may be reported with an MCACOD of 101h.

Implication: Due to this erratum, the reported MCACOD for this MCE may be incorrect.

Workaround: None identified.

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

SKW192. Executing AVX Instructions May Cause a Machine Check Error

Problem: Under complex microarchitectural conditions with Intel® HT Technology enabled, executing Intel® AVX instructions may result in Internal Timer Error in MCi_STATUS MSRs (40Dh, 411h) with MSCOD (bits [31:16]) value of 0080h and MCACOD (bits [15:0]) value of 0400h.

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

Workaround: None identified.

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

SKW193. PCIe Atomic Operation Completion TLPs May Have Non-Zero Reserved Fields

Problem: The Processor may return a non-zero value in the Lower Address field of a PCIe* Atomic Operation Completion TLP.

Implication: Due to this erratum, the processor does not fully comply with the PCIe* Completer Rules for Atomic transactions. PCIe* end-points that comply with PCIe* rules for reserved fields will ignore this value.

Workaround: None identified.

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

SKW194. Call Instruction Wrapping Around The 32-bit Address Boundary May Return to Incorrect Address

Problem: In 32-bit mode, a call instruction wrapping around the 32-bit address should save a return address near the bottom of the address space (low address) around address zero. Under complex microarchitectural conditions, a return instruction following such a call may return to the next sequential address instead (high address).

Implication: Due to this erratum, in 32-bit mode, a return following a call instruction that wraps around the 32-bit address boundary may return to the next sequential IP without wrapping around the address, possibly resulting in a #PF. Intel has not observed this behavior on any commercially available software.

Workaround: Software should not place call instructions in addresses that wrap around the 32-bit address space in 32-bit mode.

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

Specification Changes

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

- *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1: Basic Architecture*
- *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A: Instruction set reference, A-L*
- *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2B: Instruction set reference, M-U*
- *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2C: Instruction set reference, V-Z*
- *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A: System programming guide, part 1*
- *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B: System programming guide, part 2*
- *6th Generation Intel® Core™ Processor, Intel® Xeon® Processor, and Intel® Pentium® Product Families External Design Specification (EDS) - Volume 1 of 2*
- *6th Generation Intel® Core™ Processor Family and Intel® Xeon® Processor E3-1200 v5 Product Family External Design Specification (EDS) - Volume 2 of 2*

SKW1. Intel® Xeon® E3-1235L v5 and E3-1240L v5 processor ICCmax Specification to Change from 40A to 55A.

Intel will update the Intel® Xeon® E3-1235L v5 and E3-1240L v5 processors ICCmax to 55A from the current value of 40A. Recent evaluation of these products have shown, that the increased ICCmax may improve turbo residency. Current processors have been tested above this value so this change will have no negative impact.

Specification Clarifications

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

- *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 1: Basic Architecture*
- *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 2A: Instruction set reference, A-L*
- *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 2B: Instruction set reference, M-U*
- *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 2C: Instruction set reference, V-Z*
- *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3A: System programming guide, part 1*
- *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3B: System programming guide, part 2*

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

SKW1. Attempts to Simultaneously Perform Microcode Updates

Section 8.7.11 Microcode Update Resources of the *Intel® 64 and IA-32 Architectures Software Developer’s Manual*, Volume 3, will be modified to state the following:

(a) All of the microcode update steps during processor initialization should use the same update data on all threads,

(b) Any subsequent microcode update (general by an OS) must apply the same microcode update to all threads,

(c) If the processor detects an attempt to load an older microcode update in place of a newer microcode update, it may reject the older update to stay with the newer update.

Documentation Changes

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

- *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1: Basic Architecture*
- *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A: Instruction set reference, A-L*
- *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2B: Instruction set reference, M-U*
- *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2C: Instruction set reference, V-Z*
- *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A: System programming guide, part 1*
- *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B: System programming guide, part 2*

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, 2C, 3A, and 3B will be posted in a separate document, *Intel® 64 and IA-32 Architecture Software Developer's Manual Documentation Changes*. Use the following link to access this file: http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html.

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