Revision Guide for AMD Family 1Ah Models 00h-0Fh Processors

Publication Number: 58251 Revision: 1.10

Date: March 2025

AMD

List of Tables

AMD

List of Figures

Revision History

Date	Revision	Description
March 2005	1.10	Added errata #1499, #1541, #1567, #1569, #1578, #1579, #1580, #1582, #1583, #1587, and #1590.
January 2025	1.01	Initial public release.

Overview

The purpose of the *Revision Guide for AMD Family 1Ah Models 00h-0Fh* is to communicate updated product information to designers of computer systems and software developers. This revision guide includes information on the following products:

- AMD EPYC™ 9005 Series Processors

Feature support varies by brands and Ordering Part Numbers (OPNs). To determine the features supported by your processor, contact your customer representative.

This guide consists of these major sections:

- Processor Identification shows how to determine the processor revision and workaround requirements, and to construct, program, and display the processor name string.
- Product Errata provides a detailed description of product errata, including potential effects on system operation and suggested workarounds. An erratum is defined as a deviation from the product's specification, and it may cause the behavior of the processor to deviate from the published specifications.
- Documentation Support provides a listing of available technical support resources.

Revision Guide Policy

Occasionally, AMD identifies product errata that cause the processor to deviate from published specifications. Descriptions of identified product errata are designed to assist system and software designers in using the processors described in this revision guide. This revision guide may be updated periodically.

Conventions

Numbering

- **Binary numbers**. Binary numbers are indicated by appending a "b" at the end (for example, 0110b).
- **Decimal numbers**. Unless specified otherwise, all numbers are decimal. This rule does not apply to the register mnemonics.
- **Hexadecimal numbers**. Hexadecimal numbers are indicated by appending an "h" to the end, for example, 45F8h.
- **Underscores in numbers**. Underscores are used to break up numbers to make them more readable. They do not imply any operation (for example, 0110_1100b).
- **Undefined digit**. An undefined digit, in any radix, is notated as a lower case "x".

Arithmetic and Logical Operators

In this document, formulas follow some Verilog conventions as shown in Table 1.

Table 1: Arithmetic and Logic Operators

Operator	Definition
{}	Curly brackets are used to indicate a group of bits that are concatenated together. Each set of bits is separated by a comma. For example, {Addr[3:2], Xlate[3:0]} represents a 6-bit value; the two MSBs are Addr[3:2] and the four LSBs are Xlate[3:0].
|	Bitwise OR operator. For example, (01b | 10b == 11b).
||	Logical OR operator. For example, (01b || 10b == 1b); logical treats multibit operand as 1 if >=1 and produces a 1-bit result.
&	Bitwise AND operator. For example, (01b & 10b == 00b).
&&	Logical AND operator. For example, (01b && 10b == 1b); logical treats multibit operand as 1 if >=1 and produces a 1-bit result.
^	Bitwise exclusive-OR operator; sometimes used as "raised to the power of" as well, as indicated by the context in which it is used. For example, (01b ^ 10b == 11b) and (2^2 == 4).
~	Bitwise NOT operator (also known as one's complement). For example, (~10b == 01b).
!	Logical NOT operator. For example, (!10b == 0b); logical treats multibit operand as 1 if >=1 and produces a 1-bit result.
==	Logical "is equal to" operator.
!=	Logical "is not equal to" operator.

Table 1: Arithmetic and Logic Operators (continued)

Operator	Definition
<=	Less than or equal operator.
>=	Greater than or equal operator.
*	Arithmetic multiplication operator.
/	Arithmetic division operator.
<<	Shift left first operand by the number of bits specified by the 2nd operand. For example, (01b << 01b == 10b).
>>	Shift right first operand by the number of bits specified by the 2nd operand. For example, (10b >> 01b == 01b).

Register References and Mnemonics

To define errata workarounds, it is sometimes necessary to reference processor registers. References to registers in this document use a mnemonic notation consistent with that defined in the *Processor Programming Reference (PPR) for AMD Family 1Ah Model 00h-0Fh Processors*, order# 57238.

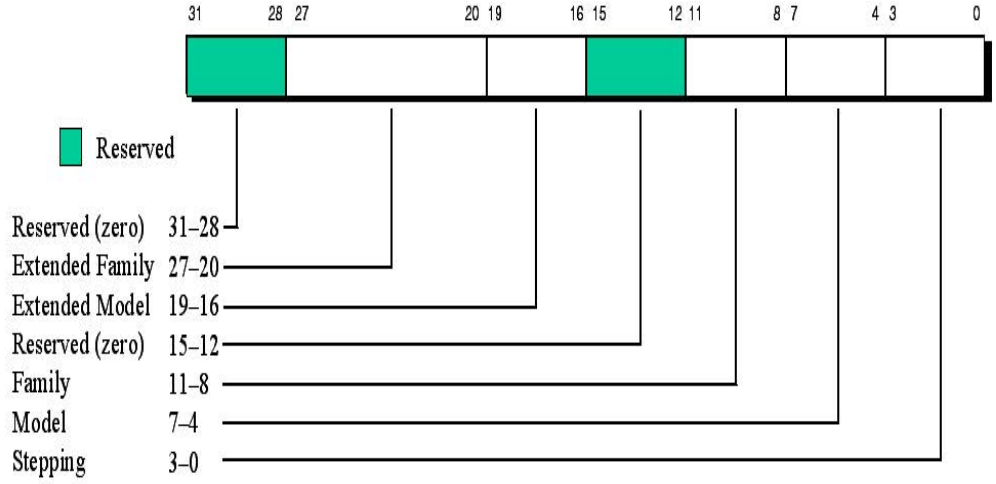
Processor Identification

This section describes how to determine the processor revision.

Revision Determination

A processor revision is identified using a unique value that is returned in the EAX register after executing the CPUID instruction function 0000_0001h (CPUID Fn0000_0001_EAX). Figure 1 shows the format of the value from CPUID Fn0000_0001_EAX.

Figure 1: Format of CPUID Fn0000_0001_EAX



The following tables show the identification numbers from CPUID Fn0000_0001_EAX for each revision of the processor to each processor segment. "X" signifies that the revision has been used in the processor segment. The absence of "X" indicates that the revision has not been used in the processor segment.

Table 2: CPUID Values for AMD Family 1Ah Models 00h-0Fh SP5 Processor Revisions

CPUID Fn0000_0001_EAX, SMUTHMx00000394 (Mnemonic)	AMD EPYC™ 9005 Series Processors
00B00F21h (Turin-Zen5-C1)	X

Programming and Displaying the Processor Name String

This section, intended for system software programmers, describes how to program and display the 48-character processor name string that is returned by CPUID Fn8000_000[4:2]. The hardware or cold reset value of the processor name string is 48 ASCII NUL characters, so system software must program the processor name string before any general purpose application or operating system software uses the extended functions that read the name string. It is common practice for system software to display the processor name string and model number whenever it displays processor information during boot up.

Note: Motherboards that do not program the proper processor name string and model number will not pass AMD validation and will not be posted on the AMD Recommended Motherboard Web site.

The name string must be ASCII NUL terminated and the 48-character maximum includes that NUL character.

The processor name string is programmed by MSR writes to the six MSR addresses covered by the range MSRC001_00[35:30]h. Refer to the PPR for the format of how the 48-character processor name string maps to the 48 bytes contained in the six 64-bit registers of MSRC001_00[35:30].

The processor name string is read by CPUID reads to a range of CPUID functions covered by CPUID Fn8000_000[4:2]. Refer to CPUID Fn8000_000[4:2] in the PPR for the 48-character processor name string mapping to the 48 bytes contained in the twelve 32-bit registers of CPUID Fn8000_000[4:2].

Operating System Visible Workarounds

This section describes how to identify operating system visible workarounds.

MSRC001_0140 OS Visible Work-around MSR0 (OSVW_ID_Length)

This register, as defined in *AMD64 Architecture Programmer's Manual Volume 2: System Programming*, order# 24593, is used to specify the number of valid status bits within the OS Visible Work-around status registers.

The reset default value of this register is 0000_0000_0000_0000h.

System software shall program the OSVW_ID_Length to 0005h prior to hand-off to the OS.

Table 3: OSVW ID Length Register

Bits	Description
63:16	Reserved.
15:0	**OSVW_ID_Length:** OS visible work-around ID length. Read-write.

MSRC001_0141 OS Visible Work-around MSR1 (OSVW_Status)

This register, as defined in *AMD64 Architecture Programmer's Manual Volume 2: System Programming*, order# 24593, provides the status of the known OS visible errata. Known errata are assigned an OSVW_ID corresponding to the bit position within the valid status field.

Operating system software should use MSRC001_0140 to determine the valid length of the bit status field. For all valid status bits:

- 1=Hardware contains the erratum, and an OS software work-around is required or may be applied instead of a system software workaround.
- 0=Hardware has corrected the erratum, so an OS software work-around is not necessary.

The reset default value of this register is 0000_0000_0000_0000h.

Table 4: OSVW Status Register

Bits	Description
63:5	**OsvwStatusBits:** Reserved. OS visible work-around status bits. Read-write.
4	**OsvwId4:** Reserved, must be zero.
3	**OsvwId3:** Reserved, must be zero.
2	**OsvwId2:** Reserved, must be zero.
1	**OsvwId1:** Reserved, must be zero.
0	**OsvwId0:** Reserved, must be zero.

System software shall program the state of the valid status bits as shown in Table 5 prior to hand-off to the OS.

Table 5: Cross Reference of Product Revision to OSVW ID

CPUID Fn0000_0001_EAX (Mnemonic)	MSRC001_0141 Bits
00B00F21h (Turin-Zen5-C1)	0000_0000_0000_0000h

Product Errata

This section documents product errata for the processors. A unique tracking number for each erratum has been assigned within this document for user convenience in tracking the errata within specific revision levels.

This table cross-references the revisions of the part to each erratum. An "X" indicates that the erratum applies to the revision. The absence of an "X" indicates that the erratum does not apply to the revision.

Note: There may be missing errata numbers. Errata that do not affect this product family do not appear. In addition, errata that have been resolved from early revisions of the processor have been deleted, and errata that have been reconsidered may have been deleted or renumbered.

Table 6: Cross-Reference of Processor Revision to Errata

No.	Errata Description	CPUID
		00B00F21h (Turin-Zen5-C1)
1155	DMA or Peer-to-peer Accesses Using Guest Physical Addresses (GPAs) May Cause IOMMU Target Abort	X
1305	AHCI Controller Ignores COMINIT During HP6: HR_AwaitAlign State	X
1464	32-Byte Misaligned Supervisor Shadow Stack Pointer or Supervisor Shadow Stack in Non-WB Memory May Result in a Non-Restartable Guest	X
1482	IBS (Instruction Based Sampling) Fetch Control Sample May Report Incorrect Page Size	X
1483	Unexpected Hardware Assert Fatal Error May Occur When Uncorrectable DRAM ECC Error Occurs	X
1489	IOMMU Unpinned Mode Is Not Supported When Secure Address Translation Service Is Enabled	X
1499	The Processor May Erroneously Compute a CS (Code Segment) Limit Violation	X
1502	HPET (High Precision Event Timer) May Increment After Enable Bit Cleared	X
1509	Certain CXL Registers Fail to Persist Through Warm Reset	X
1517	Processor May Allow Snoop While CXL WritePull or FastGo_WritePull Is Outstanding	X
1525	Systems With Incorrectly Programmed Level 1 Interrupt Table May Fail to Interrupt Guest While SEV-TIO (Secure Encrypted Virtualization - Trusted IO) Is Enabled	X

Table 6: Cross-Reference of Processor Revision to Errata (continued)

No.	Errata Description	CPUID
		00B00F21h (Turin-Zen5-C1)
1529	CXL.mem Transaction Timeout Is Not Supported	X
1533	Corrected Op Cache Tag Parity Errors May Not Be Reported	X
1534	MCA::EX::MCA_STATUS_EX[24] May be Incorrect When Reporting Watchdog Timeout Error	X
1540	Processor May Erroneously Compute a CS (Code Segment) Limit Violation in the Presence of Self-Modifying Code	X
1541	IBS (Instruction Based Sampling) Execute Sample May Capture Incorrect TLB (Translation Lookaside Buffer) Information for L1 DTLB Misses	X
1542	IBS (Instruction Based Sampling) May Erroneously Report Op Cache Miss	X
1543	IBS (Instruction Based Sampling) Sample for Speculative Fetch May Report Invalid IC Miss Flag or Physical Address	X
1544	IBS (Instruction Based Sampling) Fetch Sample May Incorrectly Report Instruction Cache Hit and Zero Latency	X
1545	PCIe® Downstream Port Containment (DPC) May Be Erroneously Triggered	X
1546	I3C® Operation at Greater Than 6MHz With More Than Four DIMMs Per I3C Bus Not Supported	X
1548	DATA_BW (Data Bandwidth) Performance Monitor Events for the CCM Interface May Undercount	X
1550	IBS (Instruction Based Sampling) Sample for Fetch May Erroneously Report Instruction Cache Miss and/or Op Cache Miss	X
1551	IBS (Instruction Based Sampling) May Report ITLB (Instruction Translation Lookaside Buffer) Hit as ITLB Miss	X
1556	Core::X86::Msr::IBS_OP_DATA3[IbsTlbRefillLat] May Be Invalid	X
1557	Core::X86::Msr::IBS_OP_DATA3[IbsDcMissLat] May Erroneously Report Non-Zero Value	X
1560	Hang May Occur If DF C-State Is Enabled and CXL® Type 1 Device Is Configured	X
1566	Stack Pointer Tracking for Dependency Removal for Add/Sub RSP Instructions May Yield Incorrect Results	X
1567	Instruction State May be Corrupted during REP CMPSB or REP SCASB	X

Table 6: Cross-Reference of Processor Revision to Errata (continued)

No.	Errata Description	CPUID
		00B00F21h (Turin-Zen5-C1)
1569	PMCx078 Counts Incorrectly in Unpredictable Ways	X
1578	Processor May Incorrectly Report CXL® Physical Layer Error (Correctable Error Status Register Bit 6)	X
1579	Guest vAPIC (Virtual Advanced Programmable Interrupt Controller) IRR (Interrupt Request Register) Backing Page May Be Corrupted	X
1580	Some PCIe® Operations Transmitting Poisoned Data Do Not Log Errors	X
1582	Processor May Report Only Lower Severity Error of Two Simultaneous Instruction Cache MCA Errors	X
1583	PMCx18E May Overcount Instruction Cache Accesses	X
1587	PMCx188 May Undercount IBS (Instruction Based Sampling) Fetch Events	X
1590	Hot Remove Event on One PCIe® Port May Cause Unexpected Completion Timeout on Another PCIe Port	X

Cross-Reference of Errata to Package Type

This table cross-references the errata to each package type. "X" signifies that the erratum applies to the package type. An empty cell signifies that the erratum does not apply. An erratum may not apply to a package type due to a specific characteristic of the erratum, or it may be due to the affected silicon revision(s) not being used in this package.

Table 7: Cross-Reference of Errata to Package Type

Errata	Package
	SP5
1155	X
1305	X
1464	X
1482	X
1483	X
1489	X
1499	X
1502	X
1509	X
1517	X
1525	X
1529	X
1533	X
1534	X
1540	X
1541	X
1542	X
1543	X
1544	X
1545	X
1546	X
1548	X

Table 7: Cross-Reference of Errata to Package Type (continued)

Errata	Package
	SP5
1550	X
1551	X
1556	X
1557	X
1560	X
1566	X
1567	X
1569	X
1578	X
1579	X
1580	X
1582	X
1583	X
1587	X
1590	X

Cross-Reference of Errata to Processor Segment

This table cross-references the errata to each processor segment. "X" signifies that the erratum applies to the processor segment. An empty cell signifies that the erratum does not apply. An erratum may not apply to a processor segment due to a specific characteristic of the erratum, or it may be due to the affected silicon revision(s) not being used in this processor segment.

Table 8: Cross-Reference of Errata to Processor Segments

Errata	Processor Segment
	AMD EPYC™ 9005 Series Processors
1155	X
1305	X
1464	X
1482	X
1483	X
1489	X
1499	X
1502	X
1509	X
1517	X
1525	X
1529	X
1533	X
1534	X
1540	X
1541	X
1542	X
1543	X
1544	X
1545	X

Table 8: Cross-Reference of Errata to Processor Segments (continued)

Errata	Processor Segment
	AMD EPYC™ 9005 Series Processors
1546	X
1548	X
1550	X
1551	X
1556	X
1557	X
1560	X
1566	X
1567	X
1569	X
1578	X
1579	X
1580	X
1582	X
1583	X
1587	X
1590	X

1155 DMA or Peer-to-peer Accesses Using Guest Physical Addresses (GPAs) May Cause IOMMU Target Abort

Description

In systems where:

- Virtualization is enabled, and
- IOMMU is in pass-through mode

DMA or peer-to-peer accesses using Guest Physical Addresses (GPAs) occurring within the regions defined below trigger a target abort.

- 0x00FD_0000_0000->0x00FD_F8FF_FFFF, or
- 0x00FD_F910_0000->0x00FD_F91F_FFFF, or
- 0x00FD_FB00_0000->0x00FD_FFFF_FFFF

Potential Effect on System

A DMA device will receive a target abort from the IOMMU.

Suggested Workaround

System software must mark the following block of memory as reserved:

- FD_0000_0000 -> FD_FFFF_FFFF

Fix Planned

No fix planned

1305 AHCI Controller Ignores COMINIT During HP6: HR_AwaitAlign State

Description

In HP6: HR_AwaitAlign state, while the AHCI controller is awaiting valid ALIGN patterns from connected SATA device, it will not respond to COMINIT issued by the connected SATA device.

Potential Effect on System

If the attached SATA device sends COMINIT instead of valid ALIGN patterns in HP6:HR_AwaitAlign state, the AHCI controller will time out awaiting valid ALIGN patterns. Consequently the AHCI controller will re-initiate Out-of-band signaling sequence at the next highest supported speed. This may result in the attached SATA device running at the lower speed.

Suggested Workaround

None

Fix Planned

No fix planned

1464 32-Byte Misaligned Supervisor Shadow Stack Pointer or Supervisor Shadow Stack in Non-WB Memory May Result in a Non-Restartable Guest

Description

Under either of the following conditions, the processor may VMEXIT a guest with the Busy Bit set in the Supervisor Shadow Stack Token while not having completed the far transfer in the guest:

- The 32 bytes of data accessed at the new supervisor shadow stack pointer are not entirely contained within one page, or
- The memory for the new supervisor shadow stack is not mapped as WB Memory.

Potential Effect on System

None expected. Software is not expected to create either of the conditions listed above. If the conditions occurred, the guest would not be able to be restarted.

Suggested Workaround

None

Fix Planned

No fix planned

1482 IBS (Instruction Based Sampling) Fetch Control Sample May Report Incorrect Page Size

Description

When a fetch is aborted, IBS (Instruction Based Sampling) may report an incorrect value for instruction cache L1TLB page size (Core::X86::Msr::IBS_FETCH_CTL[IbsL1TlbPgSz]).

Potential Effect on System

Software reading IbsL1TlbPgSz may encounter incorrect information.

Suggested Workaround

None

Fix Planned

No fix planned

1483 Unexpected Hardware Assert Fatal Error May Occur When Uncorrectable DRAM ECC Error Occurs

Description

When data poisoning is disabled, and an uncorrectable DRAM ECC error occurs, the processor will log both the expected UMC fatal error and either an unexpected CS Hardware Assert fatal error or an unexpected PIE Hardware Assert fatal error.

If a CS Hardware Assert fatal error is logged, it will have:

- MCA::CS::MCA_STATUS_CS[ErrorCodeExt] = 0x11 and
- MCA::CS::MCA_SYND_CS = 0x5D000001.

If a PIE Hardware Assert fatal error is logged, it will have:

- MCA::PIE::MCA_STATUS_PIE[ErrorCodeExt] = 0x00 and
- MCA::PIE::MCA_SYND_PIE = 0x5d002201

Potential Effect on System

Unexpected CS or PIE Hardware Assert fatal error

Suggested Workaround

None

Fix Planned

No fix planned

1489 IOMMU Unpinned Mode Is Not Supported When Secure Address Translation Service Is Enabled

Description

When Secure Address Translation Service (SATS) support is enabled (bit 31 of the IOMMU Extended Feature Register MMIO Offset 0030h is programmed to 1b), IOMMU unpinned mode (bit 187 or HPTMode of the IOMMU Device Table Entry is programmed to 1b) is not supported.

Potential Effect on System

Unpredictable device behavior

Suggested Workaround

None. Use pinned host page tables when SATS is enabled.

Fix Planned

No fix planned

1499 The Processor May Erroneously Compute a CS (Code Segment) Limit Violation

Description

The processor may erroneously compute a CS (Code Segment) limit violation under the following conditions:

- A non-flat memory model is being used.
- There is a conditional branch at the end of the code segment.
- The non-taken path violates CS limit.
- The branch is correctly predicted as taken.
- The taken branch target does not violate the CS limit.

Potential Effect on System

None expected. The violation will raise a #GP fault, however, properly written code is not expected to place a conditional branch at the end of the code segment.

Suggested Workaround

None

Fix Planned

No fix planned

1502 HPET (High Precision Event Timer) May Increment After Enable Bit Cleared

Description

After clearing the enable bit (programming FCH::TMR::HPET::HPETCONFIG[tmren] to 0b) the HPET (High Precision Event Timer) may continue to increment for up to 1.6 microseconds. During this time, back-to-back reads of the HPET may return different values, even though the operation to stop the HPET was successful.

Potential Effect on System

The HPET may appear to be incrementing after it has been disabled.

Suggested Workaround

Software should delay reading the HPET for 1.7 microseconds after disabling the HPET.

Fix Planned

No fix planned

1509 Certain CXL Registers Fail to Persist Through Warm Reset

Description

The following CXL RAS Capability Structure registers in each CXL port should persist through a warm reset but are cleared by warm reset:

- Error Capability and Control Register
- Uncorrectable Error Mask Register
- Uncorrectable Error Severity Register
- Correctable Error Mask Register

Potential Effect on System

Software may encounter incorrect debug information in the affected registers after a warm reset.

Suggested Workaround

There is no workaround for the missing debug information. It is expected that system software will re-write the control registers after a warm reset.

Fix Planned

No fix planned

1517 Processor May Allow Snoop While CXL WritePull or FastGo_WritePull Is Outstanding

Description

In violation of the CXL specification, the processor may allow a snoop to be active to the same cache line as an incoming WoWInv, WoWInvF, or WrInv CXL.Cache D2H command while the associated WritePull or FastGo_WritePull is outstanding.

Potential Effect on System

CXL Type 1 devices may observe snoop requests to the same cache line as an outstanding WritePull or FastGo_WritePull operation. CXL Type 1 devices may behave unpredictably as a result.

Suggested Workaround

None

Fix Planned

No fix planned

1525 Systems With Incorrectly Programmed Level 1 Interrupt Table May Fail to Interrupt Guest While SEV-TIO (Secure Encrypted Virtualization - Trusted IO) Is Enabled

Description

While SEV-TIO (Secure Encrypted Virtualization - Trusted IO) is enabled, the processor may fail to generate an interrupt to the guest when it processes:

- a PPR (Peripheral Page Request) from a guest, or
- a COMPLETION_WAIT command executed by a guest, or
- an event being injected into a guest event log.

The failure will not occur in systems where the Level 1 Interrupt table has been correctly programmed as described in the Extended Interrupt Remapping Table section of the AMD I/O Virtualization Technology (IOMMU) Specification.

Potential Effect on System

None expected. Systems with a correctly programmed level 1 interrupt table will not exhibit the failure. If the error occurs, then an expected interrupt may fail to be delivered.

Suggested Workaround

None

Fix Planned

No fix planned

1529 CXL.mem Transaction Timeout Is Not Supported

Description

The processor does not support CXL.mem Transaction Timeout even though the CXL.mem Transaction Timeout Supported capability bit indicates that it is supported. If CXL.mem Error Isolation is enabled, the system may unexpectedly enter CXL.mem isolation.

Potential Effect on System

System may hang or reset.

Suggested Workaround

None

Fix Planned

No fix planned

1533 Corrected Op Cache Tag Parity Errors May Not Be Reported

Description

When Correctable Op Cache Tag parity errors cause the cache access to be resynchronized and corrected, the corrected errors may not be logged in the MCA bank.

Potential Effect on System

Loss of diagnostic information for Op Cache Tag Parity Errors.

Suggested Workaround

None

Fix Planned

No fix planned

1534 MCA::EX::MCA_STATUS_EX[24] May be Incorrect When Reporting Watchdog Timeout Error

Description

MCA::EX::MCA_STATUS_EX[24] may have an erroneous value when MCA::EX::MCA_STATUS_EX[ErrorCodeExt] = 0h (Watchdog Timeout). MCA::EX::MCA_STATUS_EX[24] should be 0b when MCA::EX::MCA_STATUS_EX[ErrorCodeExt] = 0h.

The rest of the bits in the MCA::EX::MCA_STATUS_EX[AddrLsb] field are correct.

Potential Effect on System

Software reading MCA::EX::MCA_STATUS_EX after a watchdog timeout may encounter incorrect information in MCA::EX::MCA_STATUS_EX[24].

Suggested Workaround

Ignore the value of MCA::EX::MCA_STATUS_EX[24] when MCA::EX::MCA_STATUS_EX[ErrorCodeExt] = 0h, and assume MCA::EX::MCA_STATUS_EX[24] is 0b.

Fix Planned

No fix planned

1540 Processor May Erroneously Compute a CS (Code Segment) Limit Violation in the Presence of Self-Modifying Code

Description

The processor may erroneously compute a CS (Code Segment) limit violation if self-modifying code (SMC) causes an instruction which previously spanned into the next cache line and past a CS Limit to end before the CS Limit.

Potential Effect on System

A Spurious #GP fault for a CS Limit violation will be taken.

Suggested Workaround

Avoid self-modifying code that can alter the endpoint of an instruction which spans past a CS Limit boundary.

Fix Planned

No fix planned

1541 IBS (Instruction Based Sampling) Execute Sample May Capture Incorrect TLB (Translation Lookaside Buffer) Information for L1 DTLB Misses

Description

Under a highly specific and detailed set of internal timing conditions, an IBS (Instruction Based Sampling) Execute sample that has an L1 DTLB (Data Translation Lookaside Buffer) miss may capture incorrect TLB (Translation Lookaside Buffer) information. The following fields are affected:

- Core::X86::Msr::IBS_OP_DATA3[IbsTlbRefillLat]
- Core::X86::Msr::IBS_OP_DATA3[IbsDcL2TlbMiss]

Potential Effect on System

Software reading Core::X86::Msr::IBS_OP_DATA3 for an IBS Execute sample may encounter incorrect TLB information if the sample has Core::X86::Msr::IBS_OP_DATA3[IbsDcL1tlbMiss]=1.

Suggested Workaround

None

Fix Planned

No fix planned

1542 IBS (Instruction Based Sampling) May Erroneously Report Op Cache Miss

Description

When IBS (Instruction Based Sampling) reports an instruction cache miss (Core::X86::Msr::IBS_FETCH_CTL[IbsFetchIcMiss] = 1), it will also report an op cache miss (Core::X86::Msr::IBS_FETCH_CTL[IbsFetchOcMiss] = 1) whether or not there was an op cache miss.

Potential Effect on System

Software reading Core::X86::Msr::IBS_FETCH_CTL[IbsFetchOcMiss] may overcount the number of samples that miss the L1 instruction cache and miss the op cache.

Consequently, Op Cache Hits that provide all the bytes for a tagged fetch will be under-represented if their corresponding L1 Instruction Cache line is no longer resident.

IBS samples where there is an L1 IC Hit (IbsIcMiss=0) are unaffected and will correctly report the IbsFetchOcMiss state.

Suggested Workaround

None

Fix Planned

No fix planned

1543 IBS (Instruction Based Sampling) Sample for Speculative Fetch May Report Invalid IC Miss Flag or Physical Address

Description

An IBS (Instruction Based Sampling) Sample for a speculative fetch (Core::X86::Msr::IBS_FETCH_CTL[IbsFetchComp] = 0) due to a wrong older branch prediction may have incorrect values in either or both of the following fields:

- Instruction Cache Miss Flag (Core::X86::Msr::IBS_FETCH_CTL[IbsIcMiss])
- Physical address (Core::X86::Msr::IBS_FETCH_PHYSADDR[IbsFetchPhysAd])

Potential Effect on System

For an IBS sample of an aborted (Core::X86::Msr::IBS_FETCH_CTL[IbsFetchComp] = 0) speculative fetch, software may encounter incorrect values in either or both of the following fields:

- Instruction Cache Miss Flag (Core::X86::Msr::IBS_FETCH_CTL[IbsIcMiss])
- Physical address (Core::X86::Msr::IBS_FETCH_PHYSADDR[IbsFetchPhysAd])

As a result, an IBS Fetch sample may incorrectly report an IC miss as having zero latency.

Suggested Workaround

None

Fix Planned

No fix planned

1544 IBS (Instruction Based Sampling) Fetch Sample May Incorrectly Report Instruction Cache Hit and Zero Latency

Description

An IBS (Instruction Based Sampling) Sample for a fetch that aliases to an existing instruction cache entry may incorrectly report:

- Instruction Cache Miss Flag (Core::X86::Msr::IBS_FETCH_CTL[IbsIcMiss]) = 0
- Instruction Cache Fetch Latency (Core::X86::Msr::IBS_FETCH_CTL[IbsFetchLat]) = 0

Potential Effect on System

An IBS sample may incorrectly report an IC (Instruction Cache) hit and zero latency.

Suggested Workaround

None

Fix Planned

No fix planned

1545 PCIe® Downstream Port Containment (DPC) May Be Erroneously Triggered

Description

Under the following conditions, DPC (Downstream Port Containment) will erroneously be triggered for any uncorrectable RP PIO (Root Port Programmed IO) errors:

- Any RP PIO completion timeouts are unmasked (defined bits in the PCIe® RP PIO Mask Register bit programmed to 0b), and
- Any unmasked RP PIO completion timeouts are configured as uncorrectable errors (corresponding bits in PCIe RP PIO Severity Register programmed to 1b), and
- DPC triggering is not enabled (PCIe DPC Control Register[1:0] is programmed to 00b).

Potential Effect on System

None expected unless RP PIO completion timeouts are configured as uncorrectable errors and DPC triggering is not enabled.

If DPC triggering is not enabled, any RP PIO completion timeout that occurs when it is configured as uncorrectable error will unexpectedly disable the PCIe link.

Suggested Workaround

If DPC triggering is not enabled (PCIe DPC Control Register[1:0] is programmed to 00b), any unmasked RP PIO error (PCIe RP PIO Mask Register bit programmed to 0b) should have its severity set to "advisory" (corresponding PCIe RP PIO Severity Register bit programmed to 0b).

Fix Planned

No fix planned

1546 I3C® Operation at Greater Than 6MHz With More Than Four DIMMs Per I3C Bus Not Supported

Description

The processor does not support I3C® operation at greater than 6MHz with more than four DIMMs per I3C bus.

Potential Effect on System

Systems with more than four DIMMs operating the I3C bus at greater than 6MHz may experience interface errors such as DIMM detection failures or data errors on the I3C bus.

Suggested Workaround

None. Systems with more than four DIMMs per I3C bus must limit the I3C bus speed to 6MHz maximum.

Fix Planned

No fix planned

1548 DATA_BW (Data Bandwidth) Performance Monitor Events for the CCM Interface May Undercount

Description

DATA_BW (Data Bandwidth) performance monitor events for the CCM interface may undercount write bandwidth.

Potential Effect on System

Software reading the CCM data bandwidth counters may undercount write bandwidth.

Suggested Workaround

None

Fix Planned

No fix planned

1550 IBS (Instruction Based Sampling) Sample for Fetch May Erroneously Report Instruction Cache Miss and/or Op Cache Miss

Description

An IBS (Instruction Based Sampling) Sample for a fetch may erroneously report:

- An Instruction Cache Miss (Core::X86::Msr::IBS_FETCH_CTL[IbsFetchIcMiss] = 1), and/or
- An Op Cache Miss (Core::X86::Msr::IBS_FETCH_CTL[IbsFetchOcMiss] = 1).

Potential Effect on System

Overreporting of Instruction Cache Miss and/or Op Cache Miss

Suggested Workaround

None

Fix Planned

No fix planned

1551 IBS (Instruction Based Sampling) May Report ITLB (Instruction Translation Lookaside Buffer) Hit as ITLB Miss

Description

IBS (Instruction Based Sampling) may

- report a L2 ITLB (Instruction Translation Lookaside Buffer) Hit as an L2 ITLB Miss, or
- report a L2 ITLB (Instruction Translation Lookaside Buffer) Hit as an L2 ITLB Miss, and report a L1 ITLB (Instruction Translation Lookaside Buffer) Hit as an L1 ITLB Miss.

Potential Effect on System

Software may encounter an IBS sample of an ITLB access where instruction TLB miss flags (shown below) are incorrectly set:

- Core::X86::Msr::IBS_FETCH_CTL[IbsL2TlbMiss]
- Core::X86::Msr::IBS_FETCH_CTL[IbsL1TlbMiss]

This will result in the overreporting of ITLB misses.

Suggested Workaround

None

Fix Planned

No fix planned

1556 Core::X86::Msr::IBS_OP_DATA3[IbsTlbRefillLat] May Be Invalid

Description

Core::X86::Msr::IBS_OP_DATA3[IbsTlbRefillLat] may be invalid in some samples.

Potential Effect on System

Inaccuracies in performance monitoring software may be experienced.

Suggested Workaround

None.

Ignore Core::X86::Msr::IBS_OP_DATA3[IbsTlbRefillLat] in samples where Core::X86::Msr::IBS_OP_DATA3[IbsTlbRefillLat] is reported to be greater than the value of Core::X86::Msr::IBS_OP_DATA[IbsTagToRetCtr] minus the value of Core::X86::Msr::IBS_OP_DATA[IbsCompToRetCtr].

Fix Planned

No fix planned

1557 Core::X86::Msr::IBS_OP_DATA3[IbsDcMissLat] May Erroneously Report Non-Zero Value

Description

Under a highly specific and detailed set of internal timing conditions, Core::X86::Msr::IBS_OP_DATA3[IbsDcMissLat] may erroneously report a non-zero value when Core::X86::Msr::IBS_OP_DATA3[IbsDcMiss] is zero.

Potential Effect on System

Software may encounter an IBS sample where Core::X86::Msr::IBS_OP_DATA3[IbsDcMissLat] reports a non-zero value when Core::X86::Msr::IBS_OP_DATA3[IbsDcMiss] is zero.

Suggested Workaround

If Core::X86::Msr::IBS_OP_DATA3[IbsDcMiss] is zero, software should ignore the value in Core::X86::Msr::IBS_OP_DATA3[IbsDcMissLat] and assume that value is zero.

Fix Planned

No fix planned

1560 Hang May Occur If DF C-State Is Enabled and CXL® Type 1 Device Is Configured

Description

If a CXL® Type 1 device is configured in the system, and DF C-State is enabled, the CXL device or the system may hang.

Potential Effect on System

System may hang or reset.

Suggested Workaround

If a CXL Type1 device is present in the system, disable DF C-State.

System software may contain this exact workaround.

Fix Planned

No fix planned

1566 Stack Pointer Tracking for Dependency Removal for Add/Sub RSP Instructions May Yield Incorrect Results

Description

Stack Pointer Tracking for Dependency Removal for Add/Sub RSP instructions may yield incorrect results.

Potential Effect on System

Unpredictable system behavior

Suggested Workaround

System software may contain the workaround for this erratum.

Fix Planned

No fix planned

1567 Instruction State May be Corrupted during REP CMPSB or REP SCASB

Description

During the execution of a REP CMPSB or REP SCASB, the instruction state may be corrupted.

Potential Effect on System

Unpredictable system behavior

Suggested Workaround

System software may contain the workaround for this erratum.

Fix Planned

No fix planned

1569 PMCx078 Counts Incorrectly in Unpredictable Ways

Description

PMCx078 does not function correctly. It counts incorrectly in unpredictable ways.

Potential Effect on System

Inaccuracies in performance monitoring software may be experienced.

Suggested Workaround

None

Fix Planned

No fix planned

1578 Processor May Incorrectly Report CXL® Physical Layer Error (Correctable Error Status Register Bit 6)

Description

The processor may incorrectly report CXL® Physical Layer Error (Correctable Error Status Register Bit 6)

- During initial system boot, or
- In the case of non-error initiated recovery events.

Potential Effect on System

Spurious correctable error notifications and responses

Suggested Workaround

Program CXL Correctable Error Mask Register (Offset 10h) bit 6 to 1. After implementing this workaround, the processor may no longer report CXL received errors on physical layer.

To program CXL Correctable Error Mask Register (Offset 10h) bit 6 to 1, system software should program the following registers:

- CXL0x00000070[6] to 1
- CXL1x00000070[6] to 1
- CXL2x00000070[6] to 1
- CXL3x00000070[6] to 1

System software may contain the workaround for this erratum.

Fix Planned

No fix planned

1579 Guest vAPIC (Virtual Advanced Programmable Interrupt Controller) IRR (Interrupt Request Register) Backing Page May Be Corrupted

Description

Under a highly specific and detailed set of internal timing conditions, if Secure AVIC (Advanced Virtual Interrupt Controller) is enabled in a guest, the guest vAPIC (Virtual Advanced Programmable Interrupt Controller) IRR (Interrupt Request Register) backing page may be corrupted.

Potential Effect on System

Guest may miss an interrupt, or fail to clear an interrupt.

Suggested Workaround

System software may contain the workaround for this erratum.

Fix Planned

No fix planned

1580 Some PCIe® Operations Transmitting Poisoned Data Do Not Log Errors

Description

When the following PCIe® operations are transmitting poisoned data, a sync flood will occur which will prevent the poisoned data from being consumed, but no error will be logged:

- MSI (Message Signaled Interrupt)
- ATS (Address Translation Services) Page Request Message
- ATS (Address Translation Services) Invalidate Completion

Potential Effect on System

The system may hang or reset, and no error will be logged.

Suggested Workaround

None

Fix Planned

No fix planned

1582 Processor May Report Only Lower Severity Error of Two Simultaneous Instruction Cache MCA Errors

Description

Under a highly specific and detailed set of internal timing conditions, if two IC (Instruction Cache) MCA errors of the types listed below occur simultaneously, the processor may erroneously report the lower severity error rather than the higher severity error.

- MCA::IF::MCA_CTL_IF[TagMultiHit] IC Microtag or Full Tag Multi-hit Error
- MCA::IF::MCA_CTL_IF[TagParity] IC Full Tag Parity Error
- MCA::IF::MCA_CTL_IF[DataParity] IC Data Array Parity Error
- MCA::IF::MCA_CTL_IF[DqParity] Decoupling Queue PhysAddr Parity Error

Potential Effect on System

Processor may report a lower severity error while failing to report a higher severity error. The higher severity error will be handled correctly, but the diagnostic information will be missing.

Suggested Workaround

None

Fix Planned

No fix planned

1583 PMCx18E May Overcount Instruction Cache Accesses

Description

If PMCx18E[IcAccessTypes] is programmed to 18x (Instruction Cache Miss) or 1Fx (All Instruction Cache Accesses) then the performance counter may overcount.

Potential Effect on System

Inaccuracies in performance monitoring software may be experienced.

Suggested Workaround

None

Fix Planned

No fix planned

1587 PMCx188 May Undercount IBS (Instruction Based Sampling) Fetch Events

Description

If PMCx188[SampleVal] is programmed to 1b, the performance counter will undercount because it will not count aborted fetches.

Potential Effect on System

Underreporting of IBS (Instruction Based Sampling) fetch events

Suggested Workaround

None

Fix Planned

No fix planned

1590 Hot Remove Event on One PCIe® Port May Cause Unexpected Completion Timeout on Another PCIe Port

Description

An unmanaged hot remove that occurs on one port of a PCIe® root complex may cause a CTO (Completion Timeout) on a second port of the same PCIe root complex which results in DPC (Downstream Port Containment) being triggered on a second port.

This condition can only occur if an endpoint on the second port has a CTO value set to 50ms or less.

Potential Effect on System

The CTO may trigger DPC (Downstream Port Containment) which will cause a properly working endpoint to be disconnected from the PCIe link.

Suggested Workaround

If Hotplug is enabled, set the CTO value to 65ms or longer for all endpoints in the system. If an endpoint cannot be configured to have a CTO timeout of greater that 50ms then the following options are available:

- Configure the endpoint to have AER (Advanced Error Reporting) CTO be an advisory error.

Or

- Connect the endpoint to a root port within a root complex that has either:
  - No other Hotplug enabled root ports

    Or
  - No Hotpluggable endpoints attached to any Hotplug enabled root ports.

Or

- If the endpoint can internally handle any CTO as a correctable error condition, configure the endpoint to not signal CTO errors (Advanced Error Reporting CTO Mask is set to 1).

Fix Planned

No fix planned

Documentation Support

The following documents provide additional information regarding the operation of the processor:

- *AMD64 Architecture Programmer's Manual Volume 1: Application Programming*, order # 24592
- *AMD64 Architecture Programmer's Manual Volume 2: System Programming*, order # 24593
- *AMD64 Architecture Programmer's Manual Volume 3: General-Purpose and System Instructions*, order # 24594
- *AMD64 Architecture Programmer's Manual Volume 4: 128-Bit and 256-Bit Media Instructions*, order # 26568
- *AMD64 Architecture Programmer's Manual Volume 5: 64-Bit Media and x87 Floating-Point Instructions*, order # 26569
- *AMD I/O Virtualization Technology (IOMMU) Specification*, order # 48882
- *Processor Programming Reference (PPR) for AMD Family 1Ah Models 00h-0Fh Processors*, order # 57238
- *Specification for I3C® Host Controller Interface (I3C HCI℠)*

See the AMD Web site at www.amd.com for the latest updates to documents.

Notices

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. The information contained herein is subject to change and may be rendered inaccurate for many reasons, including but not limited to product and roadmap changes, component and motherboard version changes, new model and/or product releases, product differences between differing manufacturers, software changes, BIOS flashes, firmware upgrades, or the like. Any computer system has risks of security vulnerabilities that cannot be completely prevented or mitigated. AMD assumes no obligation to update or otherwise correct or revise this information. However, AMD reserves the right to revise this information and to make changes from time to time to the content hereof without obligation of AMD to notify any person of such revisions or changes.

THIS INFORMATION IS PROVIDED "AS IS." AMD MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE CONTENTS HEREOF AND ASSUMES NO RESPONSIBILITY FOR ANY INACCURACIES, ERRORS, OR OMISSIONS THAT MAY APPEAR IN THIS INFORMATION. AMD SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT WILL AMD BE LIABLE TO ANY PERSON FOR ANY RELIANCE, DIRECT, INDIRECT, SPECIAL, OR OTHER CONSEQUENTIAL DAMAGES ARISING FROM THE USE OF ANY INFORMATION CONTAINED HEREIN, EVEN IF AMD IS EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

AMD, the AMD Arrow logo, and combinations thereof are trademarks of Advanced Micro Devices, Inc.

Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies.