Arm Cortex-A78C (MP138)

Software Developer Errata Notice

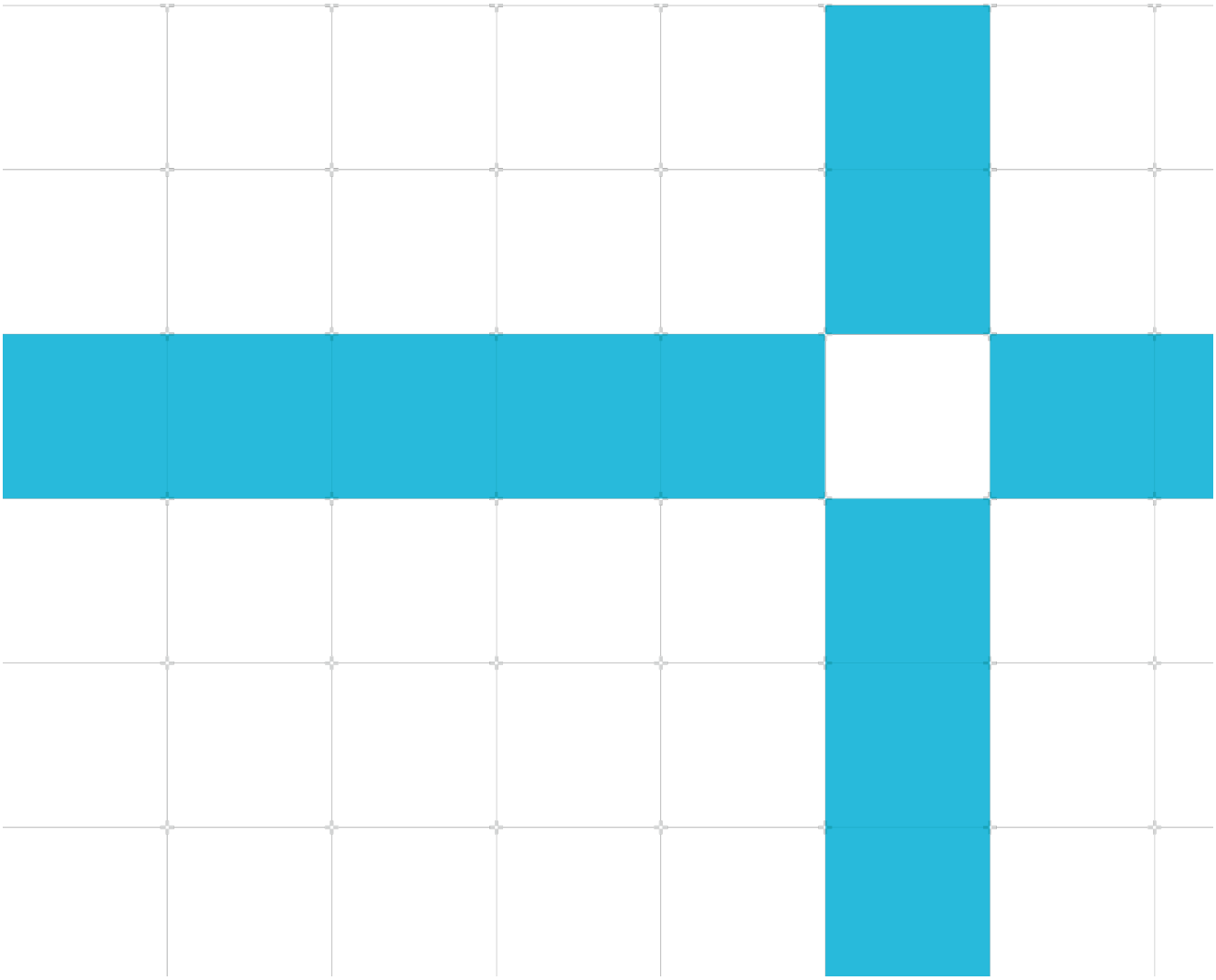
Date of issue: 23-Aug-2023

Non-Confidential

Document version: 15.0

Document ID: SDEN-1707916

This document contains all known errata since the r0p0 release of the product.



Non-confidential proprietary notice

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

(LES-PRE-20349)

Confidentiality status

This document is Non-Confidential. The right to use, copy and disclose this document may be subject to license restrictions in accordance with the terms of the agreement entered into by Arm and the party that Arm delivered this document to.

Unrestricted Access is an Arm internal classification.

Product status

The information in this document is for a product in development and is not final.

Feedback

Arm welcomes feedback on this product and its documentation. To provide feedback on Arm Cortex-A78C (MP138), create a ticket on **https://support.developer.arm.com**.

To provide feedback on the document, fill the following survey: **https://developer.arm.com/documentation-feedback-survey**.

Inclusive language commitment

Arm values inclusive communities. Arm recognizes that we and our industry have used language that can be offensive. Arm strives to lead the industry and create change.

If you find offensive language in this document, please email **terms@arm.com**.

Contents

Introduction

Scope

This document describes errata categorized by level of severity. Each description includes:

- The current status of the erratum.
- Where the implementation deviates from the specification and the conditions required for erroneous behavior to occur.
- The implications of the erratum with respect to typical applications.
- The application and limitations of a workaround where possible.

Categorization of errata

Errata are split into three levels of severity and further qualified as common or rare:

Category A	A critical error. No workaround is available or workarounds are impactful. The error is likely to be common for many systems and applications.
Category A (Rare)	A critical error. No workaround is available or workarounds are impactful. The error is likely to be rare for most systems and applications. Rare is determined by analysis, verification and usage.
Category B	A significant error or a critical error with an acceptable workaround. The error is likely to be common for many systems and applications.
Category B (Rare)	A significant error or a critical error with an acceptable workaround. The error is likely to be rare for most systems and applications. Rare is determined by analysis, verification and usage.
Category C	A minor error.

Change Control

Errata are listed in this section if they are new to the document, or marked as "updated" if there has been any change to the erratum text. Fixed errata are not shown as updated unless the erratum text has changed. The **errata summary table** identifies errata that have been fixed in each product revision.

23-Aug-2023: Changes in document version v15.0

ID	Status	Area	Category	Summary
3031176	New	Programmer	Category B	SPE might write to pages which lack write permission at Stage-1 or Stage-2
2986641	New	Programmer	Category B (rare)	PE might incorrectly detect a Watchpoint debug event instead of a Data Abort exception on a page crossing memory access, resulting in errant entry to Debug state or routing the Data Abort exception to an incorrect Exception level

22-Feb-2023: Changes in document version v14.0

ID	Status	Area	Category	Summary
2820248	New	Programmer	Category C	PE might fail to detect multiple uncorrectable ECC errors in the L1 data cache tag RAM

09-Nov-2022: Changes in document version v13.0

ID	Status	Area	Category	Summary
2743228	New	Programmer	Category B	Page crossing access that generates an MMU fault on the second page could result in a livelock
2772121	New	Programmer	Category B	The core might deadlock during powerdown sequence
2779483	New	Programmer	Category B	The PE might generate memory accesses using invalidated mappings after completion of a DVM SYNC operation
2764412	New	Programmer	Category C	Incorrect value reported for SPE PMU event 0x4000 SAMPLE_POP

04-Aug-2022: Changes in document version v12.0

ID	Status	Area	Category	Summary
2478780	New	Programmer	Category B	Pointer Authentication controls might become corrupt
2712572	New	Programmer	Category B	Core might fetch stale instruction from memory when both Stage 1 Translation and Instruction Cache are Disabled with Stage 2 forced Write-Back
2242641	New	Programmer	Category C	An SError might not be reported for an atomic store that encounters data poison
2280349	New	Programmer	Category C	PMU L1D_CACHE_REFILL_OUTER is inaccurate
2446530	New	Programmer	Category C	PMU STALL_SLOT_BACKEND and STALL_SLOT_FRONTEND events count incorrectly
2699192	New	Programmer	Category C	Incorrect value reported for SPE PMU event SAMPLE_FEED
2699198	New	Programmer	Category C	Reads of DISR_EL1 incorrectly return 0s while in Debug State
2699762	New	Programmer	Category C	Incorrect read value for Performance Monitors Control Register
2708634	New	Programmer	Category C	DRPS instruction is not treated as UNDEFINED at EL0 in Debug state
2712565	New	Programmer	Category C	Incorrect read value for Performance Monitors Configuration Register EX field

21-Jan-2022: Changes in document version v11.0

ID	Status	Area	Category	Summary
2376746	New	Programmer	Category B	Continuous failing STREX because of another PE executing prefetch for store behind consistently mispredicted branch
2395407	New	Programmer	Category B	Translation table walk folding into an L1 prefetch might cause data corruption
2341664	New	Programmer	Category C	ESR_ELx.ISV can be set incorrectly for an external abort on translation table walk
2346732	New	Programmer	Category C	Lower priority exception might be reported when abort condition is detected at both stages of translation
2423050	New	Programmer	Category C	Software-step not done after exit from Debug state with an illegal value in DSPSR

24-Sep-2021: Changes in document version v10.0

ID	Status	Area	Category	Summary
2242637	New	Programmer	Category B	PDP deadlock due to CMP/CMN + B.AL/B.NV fusion
2296015	New	Programmer	Category C	L1 Data poison is not cleared by a store

13-May-2021: Changes in document version v9.0

ID	Status	Area	Category	Summary
1875701	Updated	Programmer	Category B	Core might generate breakpoint exception on incorrect IA
2132063	New	Programmer	Category B	Disabling of data prefetcher with outstanding prefetch TLB miss might cause a deadlock
1872201	Updated	Programmer	Category C	Uncorrectable tag errors in L2 cache might cause deadlock
2004098	Updated	Programmer	Category C	DRPS might not execute correctly in Debug state with SCTLR_ELx.IESB set in the current EL
2091746	Updated	Programmer	Category C	CPU might fetch incorrect instruction from a page programmed as non-cacheable in stage-1 translation and as device memory in stage-2 translation
2102457	Updated	Programmer	Category C	ETM trace information records a branch to the next instruction as an N atom
2102759	Updated	Programmer	Category C	External APB write to a register located at offset 0x084 might incorrectly issue a write to External Debug Instruction Transfer Register
2131905	New	Programmer	Category C	Collision bit in PMBSR is reported incorrectly when there are multiple errors on SPE writes
2132043	New	Programmer	Category C	OSECCR_EL1/EDECCR is incorrectly included in the Warm Reset domain
2151898	New	Programmer	Category C	A64 WFI or A64 WFE executed in Debug state suspends execution indefinitely

03-Mar-2021: Changes in document version v8.0

ID	Status	Area	Category	Summary
2091746	New	Programmer	Category C	CPU might fetch incorrect instruction from a page programmed as non-cacheable in stage-1 translation and as device memory in stage-2 translation
2102457	New	Programmer	Category C	ETM trace information records a branch to the next instruction as an N atom
2102759	New	Programmer	Category C	External APB write to a register located at offset 0x084 might incorrectly issue a write to External Debug Instruction Transfer Register
2106992	New	Programmer	Category C	An execution of MSR instruction might not update the destination register correctly when an external debugger initiates an APB write operation to update debug registers

09-Dec-2020: Changes in document version v7.0

ID	Status	Area	Category	Summary
1875701	Updated	Programmer	Category B	Core might generate breakpoint exception on incorrect IA
1951505	Updated	Programmer	Category C	The PE might deadlock if Pseudofault Injection is enabled in Debug State

09-Nov-2020: Changes in document version v6.0

ID	Status	Area	Category	Summary
1740846	Updated	Programmer	Category B	Hardware management of dirty state and the Access flag by SPE might fail, resulting in an unsupported FSC code and incorrect EC code in PMBSR_EL1 on a buffer translation

ID	Status	Area	Category	Summary
1827430	Updated	Programmer	Category B	A transient single-bit ECC error in the MMU TC RAM might lead to stale translation in the L2 TLB
1827440	Updated	Programmer	Category B	Atomic Store instructions to shareable write-back memory might cause memory consistency failures
1875701	Updated	Programmer	Category B	Core might generate breakpoint exception on incorrect IA
1877147	Updated	Programmer	Category B	Watchpoint exception on Ld/St does not report correct address in FAR or EDWAR
1941713	Updated	Programmer	Category B	External debugger access to Debug registers might not work during Warm reset
1941499	Updated	Programmer	Category B	Store operation that encounters multiple hits in the TLB might access regions of memory with attributes that could not be accessed at that Exception level or Security state
1951501	Updated	Programmer	Category B	Atomic instructions with acquire semantics might not be ordered with respect to older stores with release semantics
2004044	New	Programmer	Category B	Virtual to physical translation latency might not be captured for SPE records when physical address collection is disabled
2004056	New	Programmer	Category B	Incorrect programming of PMBPTR_EL1 might result in a deadlock
1740836	Updated	Programmer	Category C	RAS error reported could have incorrect value in ERR0ADDR_EL1
1740844	Updated	Programmer	Category C	Instruction sampling bias exists in SPE implementation
1816420	Updated	Programmer	Category C	Loss of CTI events during warm reset
1816423	Updated	Programmer	Category C	The core might deadlock when an external debugger injects instructions using ITR register
1817660	Updated	Programmer	Category C	Possible loss of CTI event
1817664	Updated	Programmer	Category C	A memory mapped write to PMSSRR might falsely cause some PMU counters and counter overflow status to be reset after snapshot capture and read might return unknown/written data
1827435	Updated	Programmer	Category C	Watchpoint Exception on DC ZVA does not report correct address in FAR
1827438	Updated	Programmer	Category C	Memory uploads and downloads via memory access mode within Debug state can fail to accurately read or write memory contents
1872191	Updated	Programmer	Category C	External debug accesses in memory access mode with SCTLR_ELx.IESB set might result in unpredictable behavior
1872195	Updated	Programmer	Category C	Transient L2 tag double bit Errors might cause data corruption
1872198	Updated	Programmer	Category C	ERR0MISC0_EL1.SUBARRAY, ERR0STATUS.CE and ERR0STATUS.DE values for ECC errors in the L1 data cache might be incorrect
1872201	Updated	Programmer	Category C	Uncorrectable tag errors in L2 cache might cause deadlock
1941803	Updated	Programmer	Category C	PFG duplicate reported faults through a Warm reset
1941502	Updated	Programmer	Category C	L2 data RAM may fail to report corrected ECC errors
1941939	Updated	Programmer	Category C	Some corrected errors might incorrectly increment ERR0MISC0.CECR or ERR0MISC0.CECO

ID	Status	Area	Category	Summary
1951505	Updated	Programmer	Category C	The PE might deadlock if Pseudofault Injection is enabled in Debug State
1983426	New	Programmer	Category C	Incorrect fault status code might be reported in Statistical Profiling Extension register PMBSR_EL1.FSC
2004039	New	Programmer	Category C	Incorrect timestamp value reported in SPE records when timestamp capture is enabled
2004098	New	Programmer	Category C	DRPS might not execute correctly in Debug state with SCTLR_ELx.IESB set in the current EL

24-Sep-2020: Changes in document version v5.0

ID	Status	Area	Category	Summary
1941713	New	Programmer	Category B	External debugger access to Debug registers might not work during Warm reset
1941499	New	Programmer	Category B	Store operation that encounters multiple hits in the TLB might access regions of memory with attributes that could not be accessed at that Exception level or Security state
1951501	New	Programmer	Category B	Atomic instructions with acquire semantics might not be ordered with respect to older stores with release semantics
1941803	New	Programmer	Category C	PFG duplicate reported faults through a Warm reset
1941711	New	Programmer	Category C	IDATAn_EL3 might represent incorrect value after direct memory access to internal memory for Instruction TLB
1941502	New	Programmer	Category C	L2 data RAM may fail to report corrected ECC errors
1941933	New	Programmer	Category C	The core might report incorrect fetch address to FAR_ELx when the core is fetching an instruction from a virtual address associated with a page table entry which has been modified
1941936	New	Programmer	Category C	Noncompliance with prioritization of Exception Catch debug events
1941939	New	Programmer	Category C	Some corrected errors might incorrectly increment ERR0MISC0.CECR or ERR0MISC0.CECO
1951505	New	Programmer	Category C	The PE might deadlock if Pseudofault Injection is enabled in Debug State

26-Jun-2020: Changes in document version v4.0

ID	Status	Area	Category	Summary
1875701	New	Programmer	Category B	Core might generate breakpoint exception on incorrect IA
1877147	New	Programmer	Category B	Watchpoint exception on Ld/St does not report correct address in FAR or EDWAR
1872191	New	Programmer	Category C	External debug accesses in memory access mode with SCTLR_ELx.IESB set might result in unpredictable behavior
1872195	New	Programmer	Category C	Transient L2 tag double bit Errors might cause data corruption
1872198	New	Programmer	Category C	ERR0MISC0_EL1.SUBARRAY, ERR0STATUS.CE and ERR0STATUS.DE values for ECC errors in the L1 data cache might be incorrect
1872201	New	Programmer	Category C	Uncorrectable tag errors in L2 cache might cause deadlock

07-May-2020: Changes in document version v3.0

ID	Status	Area	Category	Summary
1827430	New	Programmer	Category B	A transient single-bit ECC error in the MMU TC RAM might lead to stale translation in the L2 TLB
1827440	New	Programmer	Category B	Atomic Store instructions to shareable write-back memory might cause memory consistency failures
1816420	New	Programmer	Category C	Loss of CTI events during warm reset
1816423	New	Programmer	Category C	The core might deadlock when an external debugger injects instructions using ITR register
1817660	New	Programmer	Category C	Possible loss of CTI event
1817664	New	Programmer	Category C	A memory mapped write to PMSSRR might falsely cause some PMU counters and counter overflow status to be reset after snapshot capture and read might return unknown/written data
1827435	New	Programmer	Category C	Watchpoint Exception on DC ZVA does not report correct address in FAR
1827438	New	Programmer	Category C	Memory uploads and downloads via memory access mode within Debug state can fail to accurately read or write memory contents

14-Feb-2020: Changes in document version v2.0

ID	Status	Area	Category	Summary
1740846	New	Programmer	Category B	Hardware management of dirty state and the Access flag by SPE might fail, resulting in an unsupported FSC code and incorrect EC code in PMBSR_EL1 on a buffer translation
1740836	New	Programmer	Category C	RAS error reported could have incorrect value in ERR0ADDR_EL1
1740844	New	Programmer	Category C	Instruction sampling bias exists in SPE implementation

31-Jan-2020: Changes in document version v1.0

No errata in this document version.

Errata summary table

The errata associated with this product affect the product versions described in the following table.

ID	Area	Category	Summary	Found in versions	Fixed in version
1740846	Programmer	Category B	Hardware management of dirty state and the Access flag by SPE might fail, resulting in an unsupported FSC code and incorrect EC code in PMBSR_EL1 on a buffer translation	r0p0	r0p1
1827430	Programmer	Category B	A transient single-bit ECC error in the MMU TC RAM might lead to stale translation in the L2 TLB	r0p0	r0p1
1827440	Programmer	Category B	Atomic Store instructions to shareable write-back memory might cause memory consistency failures	r0p0	r0p1
1875701	Programmer	Category B	Core might generate breakpoint exception on incorrect IA	r0p0	r0p1
1877147	Programmer	Category B	Watchpoint exception on Ld/St does not report correct address in FAR or EDWAR	r0p0	r0p1
1941499	Programmer	Category B	Store operation that encounters multiple hits in the TLB might access regions of memory with attributes that could not be accessed at that Exception level or Security state	r0p0	r0p1
1941713	Programmer	Category B	External debugger access to Debug registers might not work during Warm reset	r0p0	r0p1
1951501	Programmer	Category B	Atomic instructions with acquire semantics might not be ordered with respect to older stores with release semantics	r0p0	r0p1
2004044	Programmer	Category B	Virtual to physical translation latency might not be captured for SPE records when physical address collection is disabled	r0p0	r0p1
2004056	Programmer	Category B	Incorrect programming of PMBPTR_EL1 might result in a deadlock	r0p0	r0p1
2132063	Programmer	Category B	Disabling of data prefetcher with outstanding prefetch TLB miss might cause a deadlock	r0p0, r0p1, r0p2	Open
2242637	Programmer	Category B	PDP deadlock due to CMP/CMN + B.AL/B.NV fusion	r0p0, r0p1, r0p2	Open

ID	Area	Category	Summary	Found in versions	Fixed in version
2376746	Programmer	Category B	Continuous failing STREX because of another PE executing prefetch for store behind consistently mispredicted branch	r0p0, r0p1, r0p2	Open
2395407	Programmer	Category B	Translation table walk folding into an L1 prefetch might cause data corruption	r0p0, r0p1, r0p2	Open
2478780	Programmer	Category B	Pointer Authentication controls might become corrupt	r0p0, r0p1, r0p2	Open
2712572	Programmer	Category B	Core might fetch stale instruction from memory when both Stage 1 Translation and Instruction Cache are Disabled with Stage 2 forced Write-Back	r0p0, r0p1, r0p2	Open
2743228	Programmer	Category B	Page crossing access that generates an MMU fault on the second page could result in a livelock	r0p0, r0p1, r0p2	Open
2772121	Programmer	Category B	The core might deadlock during powerdown sequence	r0p0, r0p1, r0p2	Open
2779483	Programmer	Category B	The PE might generate memory accesses using invalidated mappings after completion of a DVM SYNC operation	r0p0, r0p1, r0p2	Open
3031176	Programmer	Category B	SPE might write to pages which lack write permission at Stage-1 or Stage-2	r0p0, r0p1, r0p2	Open
2986641	Programmer	Category B (rare)	PE might incorrectly detect a Watchpoint debug event instead of a Data Abort exception on a page crossing memory access, resulting in errant entry to Debug state or routing the Data Abort exception to an incorrect Exception level	r0p0, r0p1, r0p2	Open
1740836	Programmer	Category C	RAS error reported could have incorrect value in ERR0ADDR_EL1	r0p0	r0p1
1740844	Programmer	Category C	Instruction sampling bias exists in SPE implementation	r0p0	r0p1
1816420	Programmer	Category C	Loss of CTI events during warm reset	r0p0	r0p1
1816423	Programmer	Category C	The core might deadlock when an external debugger injects instructions using ITR register	r0p0	r0p1
1817660	Programmer	Category C	Possible loss of CTI event	r0p0	r0p1

ID	Area	Category	Summary	Found in versions	Fixed in version
1817664	Programmer	Category C	A memory mapped write to PMSSRR might falsely cause some PMU counters and counter overflow status to be reset after snapshot capture and read might return unknown/written data	r0p0	r0p1
1827435	Programmer	Category C	Watchpoint Exception on DC ZVA does not report correct address in FAR	r0p0	r0p1
1827438	Programmer	Category C	Memory uploads and downloads via memory access mode within Debug state can fail to accurately read or write memory contents	r0p0	r0p1
1872191	Programmer	Category C	External debug accesses in memory access mode with SCTLR_ELx.IESB set might result in unpredictable behavior	r0p0	r0p1
1872195	Programmer	Category C	Transient L2 tag double bit Errors might cause data corruption	r0p0	r0p1
1872198	Programmer	Category C	ERR0MISC0_EL1.SUBARRAY, ERR0STATUS.CE and ERR0STATUS.DE values for ECC errors in the L1 data cache might be incorrect	r0p0	r0p1
1872201	Programmer	Category C	Uncorrectable tag errors in L2 cache might cause deadlock	r0p0	r0p1
1941502	Programmer	Category C	L2 data RAM may fail to report corrected ECC errors	r0p0	r0p1
1941711	Programmer	Category C	IDATAn_EL3 might represent incorrect value after direct memory access to internal memory for Instruction TLB	r0p0, r0p1, r0p2	Open
1941803	Programmer	Category C	PFG duplicate reported faults through a Warm reset	r0p0	r0p1
1941933	Programmer	Category C	The core might report incorrect fetch address to FAR_ELx when the core is fetching an instruction from a virtual address associated with a page table entry which has been modified	r0p0, r0p1, r0p2	Open
1941936	Programmer	Category C	Noncompliance with prioritization of Exception Catch debug events	r0p0, r0p1, r0p2	Open
1941939	Programmer	Category C	Some corrected errors might incorrectly increment ERR0MISC0.CECR or ERR0MISC0.CECO	r0p0	r0p1

ID	Area	Category	Summary	Found in versions	Fixed in version
1951505	Programmer	Category C	The PE might deadlock if Pseudofault Injection is enabled in Debug State	r0p0	r0p1
1983426	Programmer	Category C	Incorrect fault status code might be reported in Statistical Profiling Extension register PMBSR_EL1.FSC	r0p0	r0p1
2004039	Programmer	Category C	Incorrect timestamp value reported in SPE records when timestamp capture is enabled	r0p0	r0p1
2004098	Programmer	Category C	DRPS might not execute correctly in Debug state with SCTLR_ELx.IESB set in the current EL	r0p0, r0p1	r0p2
2091746	Programmer	Category C	CPU might fetch incorrect instruction from a page programmed as non-cacheable in stage-1 translation and as device memory in stage-2 translation	r0p0, r0p1	r0p2
2102457	Programmer	Category C	ETM trace information records a branch to the next instruction as an N atom	r0p0, r0p1	r0p2
2102759	Programmer	Category C	External APB write to a register located at offset 0x084 might incorrectly issue a write to External Debug Instruction Transfer Register	r0p0, r0p1	r0p2
2106992	Programmer	Category C	An execution of MSR instruction might not update the destination register correctly when an external debugger initiates an APB write operation to update debug registers	r0p0, r0p1, r0p2	Open
2131905	Programmer	Category C	Collision bit in PMBSR is reported incorrectly when there are multiple errors on SPE writes	r0p0, r0p1	r0p2
2132043	Programmer	Category C	OSECCR_EL1/EDECCR is incorrectly included in the Warm Reset domain	r0p0, r0p1	r0p2
2151898	Programmer	Category C	A64 WFI or A64 WFE executed in Debug state suspends execution indefinitely	r0p0, r0p1, r0p2	Open
2242641	Programmer	Category C	An SError might not be reported for an atomic store that encounters data poison	r0p0, r0p1, r0p2	Open
2280349	Programmer	Category C	PMU L1D_CACHE_REFILL_OUTER is inaccurate	r0p0, r0p1, r0p2	Open
2296015	Programmer	Category C	L1 Data poison is not cleared by a store	r0p0, r0p1, r0p2	Open

ID	Area	Category	Summary	Found in versions	Fixed in version
2341664	Programmer	Category C	ESR_ELx.ISV can be set incorrectly for an external abort on translation table walk	r0p0, r0p1, r0p2	Open
2346732	Programmer	Category C	Lower priority exception might be reported when abort condition is detected at both stages of translation	r0p0, r0p1, r0p2	Open
2423050	Programmer	Category C	Software-step not done after exit from Debug state with an illegal value in DSPSR	r0p0, r0p1, r0p2	Open
2446530	Programmer	Category C	PMU STALL_SLOT_BACKEND and STALL_SLOT_FRONTEND events count incorrectly	r0p0, r0p1, r0p2	Open
2699192	Programmer	Category C	Incorrect value reported for SPE PMU event SAMPLE_FEED	r0p0, r0p1, r0p2	Open
2699198	Programmer	Category C	Reads of DISR_EL1 incorrectly return 0s while in Debug State	r0p0, r0p1, r0p2	Open
2699762	Programmer	Category C	Incorrect read value for Performance Monitors Control Register	r0p0, r0p1, r0p2	Open
2708634	Programmer	Category C	DRPS instruction is not treated as UNDEFINED at EL0 in Debug state	r0p0, r0p1, r0p2	Open
2712565	Programmer	Category C	Incorrect read value for Performance Monitors Configuration Register EX field	r0p0, r0p1, r0p2	Open
2764412	Programmer	Category C	Incorrect value reported for SPE PMU event 0x4000 SAMPLE_POP	r0p0, r0p1, r0p2	Open
2820248	Programmer	Category C	PE might fail to detect multiple uncorrectable ECC errors in the L1 data cache tag RAM	r0p0, r0p1, r0p2	Open

Errata descriptions

Category A

There are no errata in this category.

Category A (rare)

There are no errata in this category.

Category B

1740846
Hardware management of dirty state and the Access flag by SPE might fail, resulting in an unsupported FSC code and incorrect EC code in PMBSR_EL1 on a buffer translation

Status

Fault Type: Programmer Category B.
Fault Status: Present in r0p0. Fixed in r0p1.

Description

When Stage 2 dirty and access flag updates are turned off, a failed profiling buffer translation request might result in reporting a Stage 2 Data Abort code in PMBSR_EL1.EC. This also results in an Unsupported Exclusive or Atomic Access fault status code update in PMBSR_EL1, which is not one of the defined FSC codes for this register.

Configurations Affected

This erratum affects all configurations.

Conditions

SPE is enabled and the following conditions are true:

1. Hardware Management of dirty state and access flag update in Stage 1 translations is enabled in TCR_EL1.
2. Hardware Management of dirty state and access flag update in Stage 2 translations is disabled.

Implications

There might be a loss of sampling data as software needs to restart the profiling session to recover from this error.

Workaround

This erratum can be avoided by pre-dirtying the SPE buffer pages.

1827430
A transient single-bit ECC error in the MMU TC RAM might lead to stale translation in the L2 TLB

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Under certain conditions, a transient single-bit ECC error in the MMU TC RAM might prevent a TLB invalidate (TLBI) instruction from removing the entry. If the transient error is not detected for a subsequent miss request targeting the affected page, then the MMU might return a stale translation.

Configurations affected

All configurations are affected.

Conditions

All of the following conditions must be met:

1. Both stage 1 and stage 2 translations are enabled.
2. Stage 1 page or block size is larger than stage 2 page or block size.
3. MMU TC RAM entry has a transient single-bit ECC error.
4. TLBI targets the translation in the MMU TC RAM entry containing the single-bit ECC error.
5. The single-bit ECC error prevents the TLBI from removing the entry.
6. Transient single-bit ECC error goes away before a subsequent translation request matching the L2 TLB entry is issued.

Implications

If the above conditions are met, then the MMU might return stale translation for a subsequent access. The transient single-bit ECC error will be reported in ERR0MISC0_EL1 register.

Workaround

This erratum can be avoided by setting CPUECTLR_EL1[53] to 1, which disables the allocation of splintered pages in the L2 TLB.

1827440
Atomic Store instructions to shareable write-back memory might cause memory consistency failures

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Atomic Store instructions to shareable write-back memory that are performed as far atomics might cause memory consistency failures if the initiating PE has a shared copy of the cache line containing the addressed memory.

Configurations affected

This erratum affects all configurations.

Conditions

1. PE0 executes Atomic Store instruction that hits in the L1 data cache and L2 cache in the Shared state.
2. PE0 changes the L2 state to Invalid, sends an invalidating snoop to the L1 data cache, and issues a AtomicStore transaction on the CHI interconnect.
3. PE0 invalidating snoop to the L1 data cache is delayed due to internal queueing.

Implications

If the above conditions are met, PE0 might not observe invalidating snoops caused by other PEs in the same coherency domain and thus might violate memory consistency for loads to the same cache line as the Atomic Store.

Workaround

Set CPUACTLR2_EL1[2] to force Atomic Store operations to write-back memory to be performed in the L1 data cache.

1875701
Core might generate breakpoint exception on incorrect IA

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Under certain rare conditions, the core can generate a breakpoint exception on the instruction that is sequentially before the address specified in DBGBVR<n>_EL1.

Configurations Affected

This erratum affects all configurations.

Conditions

This exception might occur when:

1. Hardware breakpoint is enabled.
2. CPU instruction execution is not being single stepped.

Implications

If the above conditions are met, a breakpoint exception programmed for a given PC might instead cause a breakpoint exception for the instruction at PC-4.

Workaround

If software recognizes that a breakpoint exception has occurred for PC-4, when a breakpoint was expected at PC, then an instruction step should be performed.

Note: this erratum was previously published with a different workaround, which entailed setting CPUACTLR_EL1[21] to 1'b1. That workaround should not be applied.

1877147
Watchpoint exception on Ld/St does not report correct address in FAR or EDWAR

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

If a load or store crosses a cache line (cache line size = 64 bytes) and a watchpoint address targets a location in the upper cache line, the Fault Address Register (FAR) or the External Debug Watchpoint Address Register (EDWAR) (if set up for Debug Halt) will contain an incorrect address.

Configurations Affected

This erratum affects all configurations.

Conditions

Incorrect address in FAR or EDWAR appears when the:

1. Watchpoint targets a double word (or less or more) at cache line address B.
2. Load or store targets accesses two cache lines: lower cache line A and upper cache line B. The cache line size is 64 bytes.

Implications

FAR contains the target address of load or store.

EDWAR contains the target address of load or store if enabled for Debug Halt.

Workaround

There is no hardware workaround.

The following software workaround can be applied:

If the Fault Address Register (FAR) or External Debug Watchpoint Address Register (EDWAR) does not match a watchpoint, software can attempt to identify a relevant watchpoint:

a) For A DC ZVA whose address is not aligned to DCZID_EL0.BS by rounding the faulting address down to a cache line boundary (64 bytes) and attempting to match this against active watchpoints.

Note: most software aligns addresses used by DC ZVA, and this case is expected to be rare in practice.

b) For all other loads and stores by attempting to use the address of the next cache line boundary (64 bytes) and attempting to match this against active watchpoints.

1941499
Store operation that encounters multiple hits in the TLB might access regions of memory with attributes that could not be accessed at that Exception level or Security state

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Under certain circumstances, a store operation that encounters multiple hits in the TLB can generate a prefetch request to regions of memory with attributes that could not be accessed at that Exception level or Security state.

Configurations Affected

This erratum affects all configurations.

Conditions

1. A store operation encounters multiple hits in the TLB due to inappropriate invalidation or misprogramming of a contiguous bit.
2. A read request is generated with a physical address and attributes that are an amalgamation of the multiple TLB entries that hit.

Implications

If the above conditions are met, a read request could be generated to regions of memory with attributes that could not be accessed at that Exception level or Security state. The memory location will not be updated.

Workaround

This erratum can be avoided by setting CPUECTLR_EL1[8] to 1. There is a small performance cost (<0.5%) for setting this bit.

1941713
External debugger access to Debug registers might not work during Warm reset

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

During Warm reset, external debugger access for Debug registers might be ignored.

Configurations Affected

All configurations are affected.

Conditions

1. Warm reset is asserted.
2. External debugger access is initiated for one of following Debug registers:
    - DBGBCR<n>_EL1 (n=0-5)
    - DBGBVR<n>_EL1 (n=0-5)
    - EDECCR

Implications

If the above conditions are met, the core might ignore the access request. The read operation might return incorrect data. The write operation might not take effect and stale data might be retained.

Workaround

There is no workaround.

1951501
Atomic instructions with acquire semantics might not be ordered with respect to older stores with release semantics

Status

Fault Type: Programmer Category B.
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Under certain conditions, atomic instructions with acquire semantics might not be ordered with respect to older instructions with release semantics. The older instruction could either be a store or store atomic.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Load atomic, CAS, or SWP with acquire but no release semantics is executed.
2. There is an older instruction with release semantics and it could either be a store to non-WB memory or a store atomic instruction that is executed as a far atomic.

Implications

If the above condition are met, a memory ordering violation might happen.

Workaround

This erratum can be avoided by inserting a DMB ST before acquire atomic instructions without release semantics. This can be implemented through execution of the following code at EL3 as soon as possible after boot:

```
LDR x0,=0x0
MSR S3_6_c15_c8_0,x0
LDR x0,= 0x10E3900002
MSR S3_6_c15_c8_2,x0
LDR x0,= 0x10FFF00083
MSR S3_6_c15_c8_3,x0
LDR x0,= 0x2001003FF
MSR S3_6_c15_c8_1,x0
```

```
LDR x0,=0x1
MSR S3_6_c15_c8_0,x0
LDR x0,= 0x10E3800082
MSR S3_6_c15_c8_2,x0
LDR x0,= 0x10FFF00083
MSR S3_6_c15_c8_3,x0
LDR x0,= 0x2001003FF
MSR S3_6_c15_c8_1,x0

LDR x0,=0x2
MSR S3_6_c15_c8_0,x0
LDR x0,= 0x10E3800200
MSR S3_6_c15_c8_2,x0
LDR x0,= 0x10FFF003E0
MSR S3_6_c15_c8_3,x0
LDR x0,= 0x2001003FF
MSR S3_6_c15_c8_1,x0

ISB
```

2004044
Virtual to physical translation latency might not be captured for SPE records when physical address collection is disabled.

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Virtual address (VA) to physical address (PA) translation latency is not captured in SPE records when physical address collection is disabled at the appropriate exception level (EL).

Configurations Affected

This erratum affects all configurations.

Conditions

1. Physical address collection is disabled for SPE records at the appropriate EL by setting PMSCR_EL1.PA=0 or PMSCR_EL2.PA=0.

Implications

If the above conditions are met, then the translation latency value is not captured in the SPE records.

Workaround

Where it is acceptable to capture the physical address, this erratum can be avoided by enabling physical address sampling, by setting PMSCR_EL1.PA = 1 and PMSCR_EL2.PA = 1.

2004056
Incorrect programming of PMBPTR_EL1 might result in a deadlock

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

When PMBPTR_EL1 is incorrectly programmed to be equal to or greater than PMBLIMITR_EL1, then under certain conditions, the CPU might deadlock.

Configurations Affected

This erratum affects all configurations.

Conditions

The erratum occurs under the following conditions:

1. SPE is enabled.
2. PMBSR_EL1.S = 0, indicating PMBIRQ is not asserted.
3. PMBPTR_EL1 is programmed to be equal to or greater than PMBLIMITR_EL1.

Implications

If the above conditions are met, then the CPU might deadlock. Note that software written correctly will not expose this erratum.

Workaround

This erratum can be avoided by mediating access to the SPE control registers from a higher exception level.

A hypervisor at EL2 can configure MDCR_EL2.E2PB to trap EL1 accesses to PMBPTR_EL1, PMBLIMITR_EL1, and PMBSR_EL1. The hypervisor can mediate these accesses and maintain a shadow copy of PMBLIMITR_EL1 such that the physical PMBLIMITR_EL1 register has PMBLIMITR_EL1.E clear whenever PMBPTR_EL1.PTR >= PMBLIMITR_EL1.LIMIT.

Firmware at EL3 can configure MDCR_EL3.NSPB to disable SPE in the active security state and trap erroneous EL1/EL2 accesses to the SPE registers. Software written correctly should not access the SPE registers in this case.

2132063
Disabling of data prefetcher with outstanding prefetch TLB miss may cause a hang

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1, r0p2. Open.

Description

If the data prefetcher is disabled (by an MSR to CPUECTLR register) while a prefetch TLB miss is outstanding, the processor may hang on the next context switch.

Configurations Affected

All configurations are affected.

Conditions

- MSR write to CPUECTLR register that disables the data prefetcher.
- A TLB miss from the prefetch TLB is outstanding.

Implications

If the above conditions are met, a hang may occur on the next context switch.

Workaround

- Workaround option 1:
  If the following code surrounds the MSR, it will prevent the erratum from happening:
  - tlbi (to blind address) local version (does not have to be broadcast)
  - dsb
  - isb
  - MSR CPUECTLR - disabling the prefetcher
  - isb

- Workaround option 2:
  Place the data prefetcher in the most conservative mode instead of disabling it. This will greatly reduce prefetches but not eliminate them. This is accomplished by writing the following bits to the value indicated:
  - ecltr[7:6], PF_MODE = 2'b11

2242637
PDP deadlock due to CMP/CMN + B.AL/B.NV fusion

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1, r0p2. Open.

Description

When Performance Defined Power (PDP) is enabled, a Compare (CMP) or Compare negative (CMN) instruction followed by a conditional branch of form B.AL or B.NV might cause a deadlock.

Configurations Affected

This erratum affects all configurations.

Conditions

1. PDP configuration is enabled.
2. Execution of CMP/CMN, followed by B.AL/B.NV.

Implications

If above conditions are met, then a deadlock might result, requiring a reset of the processor.

Workaround

This erratum can be avoided by applying following patch. These instructions are not expected to be present in the code often, so any performance impact should be minimal. The code sequence should be applied early in the boot sequence prior to any of the possible errata conditions being met.

```
LDR x0,=0x5
MSR S3_6_c15_c8_0,x0 ; MSR CPUPSELR_EL3, X0
LDR x0,=0x10F600E000
MSR S3_6_c15_c8_2,x0 ; MSR CPUPOR_EL3, X0
LDR x0,=0x10FF80E000
MSR S3_6_c15_c8_3,x0 ; MSR CPUPMR_EL3, X0
LDR x0,=0x80000000003FF
MSR S3_6_c15_c8_1,x0 ; MSR CPUPCR_EL3, X0

ISB
```

Note that there is no workaround provided for r0p0 hardware. Please contact Arm support for further details.

2376746
Continuous failing STREX because of another PE executing prefetch for store behind consistently mispredicted branch

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1, r0p2. Open.

Description

A PE executing a PLDW or PRFM PST instruction that lies on a mispredicted branch path might cause a second PE executing a store exclusive to the same cache line address to fail continuously.

Configurations Affected

This erratum affects all configurations.

Conditions

1. One PE is executing store exclusive.
2. A second PE has branches that are consistently mispredicted.
3. The second PE instruction stream contains a PLDW or PRFM PST instruction on the mispredicted path that accesses the same cache line address as the store exclusive executed by the first PE.
4. PLDW/PRFM PST causes an invalidation of the first PE's caches and a loss of the exclusive monitor.

Implications

If the above conditions are met, the store exclusive instruction might continuously fail.

Workaround

Set CPUACTLR2_EL1[0] to 1 to force PLDW/PFRM ST to behave like PLD/PRFM LD and not cause invalidations to other PE caches. There might be a small performance degradation to this workaround for certain workloads that share data.

2395407
Translation table walk folding into an L1 prefetch might cause data corruption

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1, and r0p2. Open

Description

A translation table walk that matches an existing L1 prefetch with a read request outstanding on CHI might fold into the prefetch, which might lead to data corruption for a future instruction fetch.

Configurations Affected

This erratum affects all configurations

Conditions

1. In specific microarchitectural situations, the PE merges a translation table walk request with an older hardware or software prefetch L2 cache miss request.

Implications

If the previous conditions are met, an unrelated instruction fetch might observe incorrect data.

Workaround

Disable folding of demand requests into older prefetches with L2 miss requests outstanding by setting CPUACTLR2_EL1[40] to 1.

2478780
Pointer Authentication controls might become corrupt

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

When the Processing Element (PE) writes to any of the following Pointer Authentication control bits, the state of the bit might become corrupt:

- SCR_EL3.API
- HCR_EL2.API
- SCTLR_EL3.(ENDB,ENDA,ENIB,ENIA)
- SCTLR_EL2.(ENDB,ENDA,ENIB,ENIA)
- SCTLR_EL1.(ENDB,ENDA,ENIB,ENIA)

This can result in Pointer Authentication related instructions exhibiting unexpected behaviors, for example improperly executing as a NOP or failing to correctly TRAP:

- AUTDA, AUTDB, AUTDZA, AUTDZB, AUTIA, AUTIA1716, AUTIASP, AUTIAZ, AUTIB, AUTIB1716, AUTIBSP, AUTIBZ, AUTIZA, AUTIZB
- PACGA, PACDA, PACDB, PACDZA, PACDZB, PACIA, PACIA1716, PACIASP, PACIAZ, PACIB, PACIB1716, PACIBSP, PACIBZ, PACIZA, PACIZB
- RETAA, RETAB, BRAA, BRAB, BLRAA, BLRAB, BRAAZ, BRABZ, BLRAAZ, BLRABZ
- ERETAA, ERETAB, LDRAA, and LDRAB

Configurations Affected

This erratum affects all configurations.

Conditions

1. The PE writes to any of the listed Pointer Authentication control bits.
2. The PE executes a Pointer Authentication related instruction.

Implications

If the above conditions are met, then the Pointer Authentication instruction might exhibit unexpected behaviors.

Workaround

This erratum can be avoided by flushing the mop cache following a write to registers SCR_EL3, HCR_EL2, or SCTLR_ELx. This can be implemented through execution of the following code at EL3 as soon as possible after boot:

```
    LDR x0,=0x3
    MSR S3_6_c15_c8_0,x0 ; MSR CPUPSELR_EL3, X0
    LDR x0,=0xEE010F10
    MSR S3_6_c15_c8_2,x0 ; MSR CPUPOR_EL3, X0
    LDR x0,=0xFF1F0FFE
    MSR S3_6_c15_c8_3,x0 ; MSR CPUPMR_EL3, X0
    LDR x0,=0x100000004003FF
    MSR S3_6_c15_c8_1,x0 ; MSR CPUPCR_EL3, X0
    ISB
```

2712572
The core might fetch stale instruction from memory when both Stage 1 Translation and Instruction Cache are Disabled with Stage 2 forced Write-Back

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

If a core is fetching instructions from memory while stage 1 translation is disabled and instruction cache is disabled, the core ignores Stage 2 forced Write-Back indication programmed by HCR_EL2.FWB and make Non-cacheable, Normal memory request. This may cause the core to fetch stale data from memory subsystem.

Configurations Affected

This erratum might affect system configurations that do not use Arm interconnect IP.

Conditions

The erratum occurs if all the following conditions apply:

- The *Processing Element* (PE) is using EL1 translation regime.
- Stage 2 translation is enabled (HCR_EL2.VM=1).
- Stage 1 translation is disabled (SCTLR_EL1.M=0).
- Instruction cache is enabled from EL2 (HCR_EL2.ID=0).
- Instruction cache is disabled from EL1 (SCTLR_EL1.I=0).

Implications

If the conditions are satisfied, the core makes all instruction fetch request as Non-cacheable, Normal memory regardless of stage 2 translation output even if Stage 2 Forced Write-back is enabled. This might cause the core to fetch stale data from memory because Non-cacheable memory access does not probe any of cache hierarchy (e.g., Level-2 cache). If the bypassed cache hierarchy contains data modified by other initiators, stale data might be fetched from memory.

Workaround

For Hypervisor, initiating appropriate cache maintenance operations as if the core does not support stage 2 Forced Write-back feature. The cache maintenance operation should be initiated when new memory is allocated to a guest OS. This operation writeback the modified data in intermediate caches to point of coherency.

2743228
Page crossing access that generates an MMU fault on the second page could result in a livelock

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

Under unusual micro-architectural conditions, a page crossing access that generates a *Memory Management Unit* (MMU) fault on the second page can result in a livelock.

Configurations Affected

All configurations are affected.

Conditions

This erratum occurs under all of the following conditions:

1. Page crossing load or store misses in the *Translation Lookaside Buffer* (TLB) and needs a translation table walk for both pages.
2. The table walk for the second page results in an MMU fault.

Implications

If the above conditions are met, under unusual micro-architectural conditions with just the right timing, the core could enter a livelock. This is expected to be very rare and even a slight perturbation due to external events like snoops could get the core out of livelock.

Workaround

This erratum can be avoided by setting CPUACTLR5_EL1[56:55] to 2'b01.

2772121
The core might deadlock during powerdown sequence

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

While powering down the *Processing Element* (PE), a correctable L2 tag ECC error might cause a deadlock in the powerdown sequence.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. Error detection and correction is enabled through ERXCTLR_EL1.ED=1.
2. PE executes more than 24 writes to Device-nGnRnE or Device-nGnRE memory.
3. PE executes powerdown sequence as described in the *Technical Reference Manual* (TRM).

Implications

If the above conditions are met, the PE might deadlock during the hardware cache flush that automatically occurs as part of the powerdown sequence.

Workaround

Add a DSB instruction before the ISB of the powerdown code sequence specified in the TRM.

2779483
The PE might generate memory accesses using invalidated mappings after completion of a DVM SYNC operation

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1, r0p2. Open.

Description

The Processing Element (PE) might generate memory accesses using invalidated mappings after completion of a Distributed Virtual Memory (DVM) SYNC operation.

Configurations Affected

All configurations are affected.

Conditions

This erratum can occur on a PE (PE0) only if the affected TLBI and subsequent DVM sync operations are broadcast from another PE (PE1). The TLBI and DVM sync operations executed locally by PE0 are not affected.

Implications

When this erratum occurs, after completion of a DVM SYNC operation, the PE can continue generating memory accesses through mappings that were invalidated by a previous TLBI operation.

Workaround

The erratum can be avoided by setting CPUACTLR3_EL1[47]. Setting this chicken bit might have a small impact on power and negligible impact on performance.

3031176
SPE might write to pages which lack write permission at Stage-1 or Stage-2

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1 and r0p2. Open.

Description

The *Statistical Profiling Extension* (SPE) uses the Stage-1 translation regime of the owning exception level in the owning Security state. Due to this erratum, the SPE might write to memory which lacks write permission at Stage-1 and/or Stage-2 of the owning exception level's translation regime, without raising a fault.

Configurations affected

This erratum affects all configurations that support SPE.

Conditions

This erratum occurs under the following conditions:

1. The SPE buffer is enabled.
2. Registers PMBPTR_EL1 and PMBLIMITR_EL1 are configured to include a virtual address VA_X.
3. A valid Stage-1 translation exists for the virtual address VA_X.
4. If Stage-2 is enabled, a valid Stage-2 translation exists for the intermediate physical address IPA_X for the virtual address VA_X.
5. At least one of the following conditions is true:
   a. The Stage-1 translation for VA_X lacks write permission.
   b. The Stage-2 translation for IPA_X lacks write permission.
6. None of the following apply:
   a. Stage-1 hardware dirty bit management is enabled.
   b. Stage-2 is enabled, and Stage-2 hardware dirty bit management is enabled.

Implications

The SPE might write to VA_X rather than generating a fault. This might allow malicious software with control over SPE to corrupt memory for which it is not intended to have write access to.

Workaround

No hardware workaround is available.

A hypervisor at EL2 should not give virtual machines control of SPE unless the hypervisor can handle writes to any pages mapped at Stage-2.

An OS kernel at EL1 or EL2 should not configure the SPE buffer to contain any page which might lack write permission at Stage-1.

No current software is expected to have this problem.

Category B (rare)

2986641
PE might incorrectly detect a Watchpoint debug event instead of a Data Abort exception on a page crossing memory access, resulting in errant entry to Debug state or routing the Data Abort exception to an incorrect Exception level

Status

Fault Type: Programmer Category B (Rare)
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

Under certain conditions, the *Processing Element* (PE) might incorrectly detect a Watchpoint debug event instead of a Data Abort exception when a memory access spans multiple pages. The Data Abort is detected for the first page and the Watchpoint debug event is associated with the second page. The Watchpoint debug event detection might route the Data Abort to the incorrect target Exception level or cause the PE to enter Debug state.

Note the contents of the ESR and FAR registers capture the information associated with the Data Abort.

Configurations affected

This erratum affects all configurations.

Conditions

1. Watchpoints are enabled.
2. The PE executes a page split access that generates a Data Abort on the first page and a Watchpoint match on the second page.
3. The PE executes a younger load instruction that generates an external abort which coincides with a 1 cycle window when processing the Data Abort and Wathchpoint debug event.

Implications

If the previous conditions are met and EDSCR.HDE is set (enables Halting Debug on Watchpoint debug event), then the PE will enter Debug state rather than taking a Data Abort exception.

If EDSCR.HDE is not set, the PE might route the abort to the incorrect Exception level:

- If MDCR_EL2.TDE == 0, a stage 2 Data Abort might result in a Data Abort exception taken erroneously to EL1.

    - The rarity of PE internal timings required to exhibit this bug is comparable to *Reliability, Availability, and Serviceability* (RAS) error FIT rates. Expected outcome is a kernel panic that will kill the process.
- If MDCR_EL2.TDE == 1, a stage 1 Data Abort might result in a Data Abort exception taken erroneously to EL2.
    - This scenario is containable within a hypervisor via the software workaround outlined below.

Workaround

There is no complete workaround for this erratum. A partial software workaround addresses the more serious scenario of a stage 1 Data Abort resulting in a Data Abort exception taken erroneously to EL2 without updating HPFAR_EL2.

EL2 can protect against this case as follows:

- Reserve one bit of IPA space so that VTCR_EL2.PS is never the maximum supported.
- Write all 1's to HPFAR_EL2[63:0] before entering EL1 or EL0.
- Exceptions to EL2 due to this erratum that should have set HPFAR_EL2 will instead use an out of range IPA. The guest should be restarted as the conditions for this erratum are rare and are not likely to be encountered again.

Category C

1740836
RAS error reported could have incorrect value in ERR0ADDR_EL1

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Under certain conditions, capacity eviction of a line which single or double bit ECC error is in the process of being reported could end up corrupting the value in ERR0ADDR_EL1 register.

Configurations Affected

The erratum affects configurations with CORE_CACHE_PROTECTION set to TRUE.

Conditions

1. ECC error is detected in the L1 Data RAM.
2. RAS error is in the process of being reported and the line is replaced due to capacity eviction.

Implications

If the above conditions are met, ERR0ADDR_EL1 could have incorrect value. In the case of a single bit error, the data will be corrected and in the case of a double bit error data is written out as poisoned.

Workaround

There is no workaround for this erratum.

1740844
Instruction sampling bias exists in SPE implementation

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

A PE that is used to perform instruction sampling using the SPE mechanism might exhibit sampling bias toward instructions that are branch targets.

Configurations Affected

This erratum affects all configurations.

Conditions

1. SPE configured and utilized on PE.

Implications

Software utilizing SPE might see unexpectedly high sample counts for branch target instructions and unexpectedly low sample counts for some instructions closely following a branch target.

Workaround

No hardware workaround.

1816420
Loss of CTI events during warm reset

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

ETM external output CTI events from the core to the external DebugBlock will not be reported during warm reset.

Configurations affected

This erratum affects all configurations.

Conditions

1. An ETM external output CTI event occurs while warm reset is asserted.

Implications

The ETM external output CTI event will be dropped and any cross triggering that depends on this CTI event will not occur. For example, if the ETM external output was to be used to trigger a trace capture component to stop trace capture, then trace capture will not stop due to this event.

Workaround

This erratum has no workaround.

1816423
The core might deadlock when an external debugger injects instructions using ITR register

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

The core might deadlock when an external debugger injects instructions by ITR register.

Configurations affected

This erratum affects all configurations.

Conditions

1. An external debugger requests the core to enter debug state while the core is stalled because of an instruction abort due to a permission fault.
2. The external debugger injects instructions using the ITR register.

Implications

The core might deadlock if the above conditions are satisfied.

Workaround

This erratum has no workaround.

1817660
Possible loss of CTI event

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

A CTI event from the core to the external DebugBlock might be dropped, in rare occurrences, if close in temporal proximity to a previous CTI event.

Configurations affected

This erratum affects all configurations.

Conditions

1. CTI event occurs.
2. Another CTI event occurs before completion of the processing of the previous CTI event.

Implications

CTI events might be dropped.

Workaround

This erratum has no workaround.

1817664
A memory mapped write to PMSSRR might falsely cause some PMU counters and counter overflow status to be reset after snapshot capture and read might return unknown/written data

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description:

A memory mapped write to PMSSRR at offset 0x6f4 might configure the Cycle counter and/or Performance Monitor event counters to be reset along with reset of corresponding overflow status bits in the PMOVSR register. The register supports read/write functionality instead of RAZ/WI.

Configurations affected

This erratum affects all configurations.

Conditions

1. System enables PMU snapshot mechanism.
2. System performs memory mapped write of PMSSRR setting PMSSRR[x], where x is 31 or any value from 0 to 5 (inclusive).
3. Snapshot trigger is seen through a legal mechanism.

Implications

If the above conditions are met, the corresponding counter (PMCCNTR_EL0 if x=31 or PMEVCNTR<x>_EL0 if x = [0,5]) will reset after a snapshot is taken. Further, the corresponding bit in the PMOVSR_EL0 register will be reset.

A memory mapped read will return data that is written to these bits and 0 otherwise.

This register is supposed to have RAZ/WI functionality and no effect on other counters.

Workaround

Avoid write of PMSSRR when system is using the PMU Snapshot mechanism.

1827435
Watchpoint Exception on DC ZVA does not report correct address in FAR

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

If the watchpoint address targets a lower portion of a cache line, but not all of the cache line, and the address target of the DC ZVA falls in the upper portion of the cache line that the watchpoint does not target the FAR will contain an incorrect address.

Configurations affected

This erratum affects all configurations.

Conditions

1. Watchpoint targets double word (or less or more) at address A.
2. DC ZVA targets address greater than A+7, but less than A+63. The cache line size is 64 bytes, which is a mis-aligned address.

Implications:

FAR contains target address of DC ZVA.

Workaround:

There is no hardware workaround. The common case for DC ZVA targets is to be granule aligned, thus most software will not be affected by this case.

1827438
Memory uploads and downloads via memory access mode within Debug state can fail to accurately read or write memory contents

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Memory uploads via memory access mode within Debug state might fail to set EDSCR.TXfull to 1, possibly resulting in an intended memory read being skipped and erroneous memory contents being displayed for that address.

Memory downloads via memory access mode within Debug state might prematurely clear EDSCR.RXfull, possibly resulting in an intended memory write being skipped and subsequent memory access mode downloads therefore writing data to incorrect addresses.

Configurations affected

This erratum affects all configurations.

Conditions

For memory upload:

1. The core is in Debug state having been properly set up via the external debug interface for memory upload (target to external host).
2. A series of external reads from DBGDTRTX_EL0 are used, where each read first clears EDSCR.TXfull to 0, then initiates memory uploads via PE-generated load & system register write instruction pairs, then sets EDSCR.(TXfull,ITE) to (1,1) on successful completion of each iteration.
3. Certain internal timing conditions relating to execution of a previous load instruction exist, resulting in the failure to set EDSCR.TXfull to 1 on some iteration.

For memory download:

1. The core is in Debug state having been properly set up via the external debug interface for memory download (external host to target).
2. A series of external writes to DBGDTRRX_EL0 are used, where each write first sets EDSCR.RXfull to 1, then initiates memory downloads via PE-generated system register read & store instruction pairs, then sets EDSCR.(RXfull,ITE) to (0,1) on successful completion of each iteration.
3. Certain internal timing conditions relating to execution of a previous load instruction exist, resulting in a premature clearing of EDSCR.RXfull to 0 on some iteration.

Implications

If the above conditions are met, the failure mechanism could effectively skip an intended memory read in a memory upload loop, thus resulting in the erroneous display of data associated with the affected memory address. Or, the failure mechanism could effectively skip an intended memory write in a memory download loop, thus resulting in subsequent memory access mode downloads writing data to incorrect addresses.

Workaround

A workaround is only needed if there is any possibility of connecting an external debugger to the core. If that possibility exists, then there are 2 separate workarounds:

1. Perform the memory upload or download operations with the debugger's FAST_MEMORY_ACCESS disabled. This can impact the performance of memory upload and download operations in Debug state, resulting in slight visible delays in the debugger user interface on memory upload and longer download times.
   or
2. Set CPUACTLR3_EL1[47] in the boot sequence to prevent the faulty behavior. There is no performance impact associated with setting this bit, but there is a potential (workload dependent) power increase of approximately 1.5% total core power.

1872191
External debug accesses in memory access mode with SCTLR_ELx.IESB set might result in unpredictable behavior

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

In Debug state with SCTLR_ELx.IESB set to 1, memory uploads and downloads executed in memory access mode might lead to unpredictable behavior for the current exception level.

Configurations affected

This erratum affects all configurations.

Conditions

1. Core is In Debug state.
2. SCTLR_ELx.IESB is set to 1 for the current exception level.
3. Memory access mode is enabled via EDSCR.MA set to 1.

Implications

If the above conditions are met, memory upload and download behavior is unpredictable for the current exception level and might lead to incorrect operation or results. The unpredictable behavior is limited to legal behavior at the current exception level.

Workaround

The erratum can be avoided by clearing SCTLR_ELx.IESB before performing memory uploads or downloads in Debug state using memory access mode.

1872195
Transient L2 tag double bit Errors might cause data corruption

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Under certain uncommon conditions, transient double bit tag errors might cause valid cache data that is in an unrelated line in the same set to be overwritten.

Configurations affected

All configurations with CORE_CACHE_PROTECTION enabled.

Conditions

The following conditions must be met during additional rare timing and state conditions:

1. A double bit error (DBE) in the tag occurs shortly after the read of a line.
2. The DBE occurs before a write to that same line in a different way.
3. The DBE corrects after the write to that line.
4. An additional read is made to that line before it is evicted from the cache.

Implications

If the above conditions are met, the data in an unrelated line in the same set might be overwritten and corrupted. The effect on the failure rate is negligible in such a case. There is still substantial benefit being gained from the ECC logic.

Workaround

There is no workaround.

1872198
ERR0MISC0_EL1.SUBARRAY, ERR0STATUS.CE and ERR0STATUS.DE values for ECC errors in the L1 data cache might be incorrect

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Under certain conditions, the ERR0MISC0_EL1.SUBARRAY, ERR0STATUS.CE and ERR0STATUS.DE values recorded for ECC errors in the L1 data cache might be incorrect.

Configurations affected

This erratum affects configurations with CORE_CACHE_PROTECTION set to TRUE.

Conditions

1. The L1 data cache contains both a single-bit and double-bit ECC error on different words within the same 64-byte cacheline.
2. An access is made to the cacheline in the L1 data cache containing both the single-bit and double-bit ECC errors simultaneously.

Implications

If the above conditions are met, then ERR0MISC0_EL1.SUBARRAY, ERR0STATUS.CE and ERR0STATUS.DE might have an incorrect values.

Workaround

There is no workaround for this erratum.

1872201
Uncorrectable tag errors in L2 cache might cause deadlock

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Under rare conditions that include the aliasing of multiple virtual addresses to a single physical address, a detected and reported double-bit ECC error in the L2 cache tag RAM might lead to a state in which an unexpected L1 cache eviction can cause a deadlock in the L2 cache.

Configurations affected

This erratum affects configurations with CORE_CACHE_PROTECTION TRUE.

Conditions

1. L2 cache detects and reports a tag double-bit ECC error.
2. A set of rare conditions occur within the PE's memory system.

Implications

If the above conditions are met, the L2 transaction queue might deadlock and never complete the prefetch operation.

Workaround

There is no workaround for this erratum.

1941502
L2 data RAM may fail to report corrected ECC errors

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

For specific operation types and cache states, a read of the L2 data RAM might fail to report a detected and corrected single-bit ECC error.

Configurations Affected

All configurations are affected.

Conditions

1. PE L1 data cache and L2 cache are in a SharedClean state and the exclusive monitor is armed for a given physical address.
2. PE executes a store exclusive instruction to this physical address.
3. L2 cache reads its data RAMs, and detects and corrects a single-bit ECC error.

Implications

If the above conditions are met, the PE will correct the error, but might fail to report it in the RAS error log registers. This can cause a small loss in diagnostic capability.

Workaround

There is no workaround.

1941711
IDATAn_EL3 might represent incorrect value after direct memory access to internal memory for Instruction TLB

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2. Open.

Description

After implementation-defined RAMINDEX register is programmed to initiate direct memory access to internal memory for Instruction TLB, implementation-defined IDATAn_EL3 value represents unpredictable value.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Implementation-defined RAMINDEX register is programmed to initiate direct memory access to internal memory for Instruction TLB.

Implications

If the above conditions are met, IDATAn_EL3 register might represent incorrect value for Translation regime, VMID, ASID, and VA[48:21].

Workaround

There is no workaround.

1941803
PFG duplicate reported faults through a Warm reset

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

In certain conditions, the Pseudo-fault Generation Error Record Registers might generate duplicate faults through a Warm reset.

Configurations Affected

This erratum affects all configurations.

Conditions

1. ERR0PFGCDN is set with a non-zero countdown value.
2. ERR0PFGCTL is set to generate a pseudo-fault with ERR0PFGCTL.CDEN enabled.
3. The countdown value expires, generating a pseudo-fault.
4. Warm reset asserts.

Implications

After the Warm reset, a second generated pseudo-fault might occur.

Workaround

De-assert the ERR0PFGCTL control bits before asserting a Warm reset.

1941933
The core might report incorrect fetch address to FAR_ELx when the core is fetching an instruction from a virtual address associated with a page table entry which has been modified

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2. Open.

Description

When a core fetches an instruction from a virtual address that is associated with a page table entry which has been modified and the fetched block is affected by parity error, the core might report an incorrect address within the same 32B block onto the Fault Address Register (FAR).

Configurations Affected

All configurations are affected.

Conditions

1. The core fetches instructions from an aligned 32B virtual address block.
2. A page table entry associated with the above 32B aligned block is updated. The new translation would cause an instruction abort.
3. TLB holds the old translation since the synchronization process, for example, TLB Invalidate (TLBI) followed by Data Synchronization Barrier (DSB), was not completed.
4. Some of the fetched instructions are affected by parity error in I-cache data RAM.
5. Context synchronization events were not processed between the last executed instruction and the above instruction.

Implications

When above conditions are satisfied, a core might report an incorrect fetch address to FAR_ELx. The address reported in FAR_ELx points at an earlier location in the same aligned 32B block. FAR_ELx[63:5] still points correct virtual address.

Workaround

There is no workaround.

1941936
Noncompliance with prioritization of Exception Catch debug events

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2. Open.

Description

ARMv8.2 architecture requires that Debug state entry due to an Exception Catch debug event (generated on exception entry) occur before any asynchronous exception is taken at the first instruction in the exception handler. An asynchronous exception might be taken as a higher priority exception than Exception Catch and the Exception Catch might be missed altogether.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Debug Halting is allowed.
2. EDECCR bits are configured to catch exception entry to ELx.
3. A first exception is taken resulting in entry to ELx.
4. A second, asynchronous exception becomes visible at the same time as exception entry to ELx.
5. The second, asynchronous exception targets an Exception level ELy that is higher than ELx.

Implications

If the above conditions are met, the core might recognize the second exception and not enter Debug state as a result of Exception Catch on the first exception. When the handler for the second exception completes, software might return to execute the first exception handler, and assuming the core does not halt for any other reason, the first exception handler will be executed and entry to Debug state via Exception Catch will not occur.

Workaround

When setting Exception Catch on exceptions taken to an Exception level ELx, the debugger should do either or both of the following:

1. Ensure that Exception Catch is also set for exceptions taken to all higher Exception Levels, so that the second (asynchronous) exception generates an Exception Catch debug event.
2. Set Exception Catch for an Exception Return to ELx, so that when the second (asynchronous)

exception handler completes, the exception return to ELx generates an Exception Catch debug event.

Additionally, when a debugger detects that the core has halted on an Exception Catch to an Exception level ELy, where y > x, it should check the ELR_ELy and SPSR_ELy values to determine whether the exception was taken on an ELx exception vector address, meaning an Exception Catch on entry to ELx has been missed.

1941939
Some corrected errors might incorrectly increment ERR0MISC0.CECR or ERR0MISC0.CECO

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

If a Corrected Error is recorded because of a bus error which has no valid location (ERR0STATUS.MV=0x0), then a subsequent Corrected Error might incorrectly increment either of the ERR0MISC0.CECR or ERR0MISC0.CECO counters.

Configurations Affected

This erratum affects all configurations.

Conditions

1. A Corrected Error which has no valid location (ERR0STATUS.MV=0x0) is recorded.
2. A subsequent Corrected Error occurs.

Implications

The subsequent Corrected Error might improperly increment either of the ERR0MISC0.CECR or ERR0MISC0.CECO counters.

Workaround

No workaround is expected to be required.

1951505
The PE might deadlock if Pseudofault Injection is enabled in Debug State

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

If Pseudofault Injection is enabled for the PE node (ERR0PFGCTL.CDNEN=0x1) and the PE subsequently enters Debug State, then the PE might deadlock. Alternatively, if the PE is executing in Debug State and the PE enables Pseudofault Injection for the PE node (ERR0PFGCTL.CDNEN=0x1), then the PE might deadlock.

Configurations Affected

This erratum affects all configurations.

Conditions

1. ERR0PFGCTL.CDNEN is set to 0x1 to enable Pseudofault Injection.
2. The PE enters Debug State.

OR

1. The PE is executing in Debug State.
2. ERR0PFGCTL.CDNEN is set to 0x1 to enable Pseudofault Injection.

Implications

If the above conditions are met, then the PE might deadlock.

Workaround

Ensure ERR0PFGCTL.CDNEN=0x0 before entering Debug State and while executing in Debug State.

1983426
Incorrect fault status code might be reported in Statistical Profiling Extension register PMBSR_EL1.FSC

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

A statistical profiling buffer translation request which encounters multiple hits in the TLB might report an incorrect fault status code in PMBSR_EL1.FSC.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Statistical Profiling Extension (SPE) is enabled.
2. A translation request is made for the statistical profiling buffer.
3. This translation request encounters multiple hits in the TLB due to incorrect invalidation or misprogramming of translation table entries.

Implications

If the above conditions are met, then the fault status code reported in PMBSR_EL1.FSC might incorrectly indicate an illegal or incorrect fault status code instead of the correct TLB Conflict fault code.

Workaround

There is no workaround.

2004039
Incorrect timestamp value reported in SPE records when timestamp capture is enabled

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

The timestamp value that is captured in SPE records is from when the SPE record is written out to L2, as opposed to before the operation is signaled as "complete".

Configurations Affected

This erratum affects all configurations.

Conditions

1. Timestamp capture is enabled for SPE records at the appropriate EL by setting PMSCR_EL1.TS or PMSCR_EL2.TS.

Implications

If the above conditions are met, then the timestamp value reported in the SPE records might be outside of the sampled operation's lifetime.

For most expected use cases, the inaccuracy is not expected to be significant.

Workaround

There is no workaround.

2004098
DRPS might not execute correctly in Debug state with SCTLR_ELx.IESB set in the current EL

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1. Fixed in r0p2.

Description

In Debug state with SCTLR_ELx.IESB set to 1, the **`DRPS`** (debug only) instruction does not execute properly. Only partial functionality of the **`DRPS`** instruction is performed.

Configurations Affected

This erratum affects all configurations.

Conditions

The erratum occurs under the following conditions:

1. The core is in Debug state.
2. SCTLR_ELx.IESB is set to 1 for the current exception level.
3. The **`DRPS`** instruction is executed.

Implications

If the above conditions are met, the **`DRPS`** instruction does not complete as intended, which might lead to incorrect operation or results. Register data or memory will not be corrupted. There are also no security or privilege violations.

Workaround

The erratum can be avoided by clearing SCTLR_ELx.IESB followed by the insertion of an **`ISB`** and an **`ESB`** instruction in code before the **`DRPS`** instruction.

2091746
CPU might fetch incorrect instruction from a page programmed as non-cacheable in stage-1 translation and as device memory in stage-2 translation

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1. Fixed in r0p2.

Description

When an instruction fetch is initiated for a page programmed as non-cacheable normal memory in stage-1 translation and as device memory in stage-2 translation, the instruction memory might incorrectly return 0. This might cause an unexpected UNDEFINED exception.

Configurations Affected

The erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. A CPU fetch instruction from a page satisfies the following:
    - Stage-1 translation of this page is programmed as non-cacheable normal memory.
    - Stage-2 translation of this page is programmed as device memory.

Implications

If the above conditions are met, the CPU might read 0 from the instruction memory. This instruction might cause an unexpected UNDEFINED exception. Instruction fetches to device memory are not architecturally predictable in any case, and device memory is expected to be marked as execute never, so this erratum is not expected to cause any problems to real-world software.

Workaround

This erratum has no workaround.

2102457
ETM trace information records a branch to the next instruction as an N atom

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1. Fixed in r0p2.

Description

If a branch is taken to the next instruction, and if the instruction state remains the same, then the ETM traces it as an N atom rather than an E atom or branch address packet. This is incorrect as the ETM architecture says a taken branch should be traced as an E atom. This affects all forms of branches. State-changing branches are traced correctly.

Configurations Affected

This erratum affects all configurations.

Conditions

This issue might occur when:

1. ETM is enabled.
2. A branch is taken to the next instruction.
3. The instruction state does not change.

Implications

A trace decoder that interprets an N atom to move to the next instruction in the same state without a push or pop from the return stack will correctly maintain the control flow but will not be able to infer anything from a conditional branch.

A trace decoder that checks if unconditional branches were not traced as N atom might report an error.

Workaround

To ensure continued control flow, ensure the trace decoder always interprets an N atom to move to the next instruction in same state without a push or pop from the return stack.

2102759
External APB write to a register located at offset 0x084 might incorrectly issue a write to External Debug Instruction Transfer Register

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1. Fixed in r0p2.

Description

The core might incorrectly issue a write to External Debug Instruction Transfer Register (EDITR) when an external APB write to another register that is located at offset 0x084 is performed in the Debug state. The following debug components share the offset alias with the EDITR register:

- ETE - TRCVIIECTLR - ViewInst Include/Exclude Control Register
- Reserved locations

Configurations Affected

This erratum affects all configurations.

Conditions

1. The core is in debug state.
2. The External Debug Status and Control Register (EDSCR) cumulative error flag field is 0b0.
3. Memory access mode is disabled, in example, EDSCR.MA = 0b0.
4. The OS Lock is unlocked.
5. External APB write is performed to a memory mapped register at offset 0x084 other than the EDITR.

Implications

If the above conditions are met, then the core might issue a write to the EDITR and try to execute the instruction pointed to by the ITR. As a result of the execution, the following might happen:

- CPU state and/or memory might get corrupted.
- The CPU might generate an UNDEFINED exception.
- The EDSCR.ITE bit will be set to 0.

Workaround

Before programming any register at this offset when the PE is in Debug state, the debugger should either:

- Set the EDSCR.ERR bit by executing some Undefined instruction (e.g. writing zero to EDITR); or
- Set the OS Lock and then unlock it afterwards.

2106992
An execution of MSR instruction might not update the destination register correctly when an external debugger initiates an APB write operation to update debug registers

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2. Open.

Description

When an **MSR** instruction and an APB write operation are processed on the same cycle, the **MSR** instruction might not update the destination register correctly.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. A CPU executes an **MSR** instruction to update any of following SPR registers:
   a. DBGBCR<n>_EL1
   b. DBGBVR<n>_EL1
   c. DBGWCR<n>_EL1
   d. DBGWVR<n>_EL1
   e. OSECCR_EL1
2. An external debugger initiates an APB write operation for any of following registers:
   a. DBGBCR<n>
   b. DBGBVR<n>
   c. DBGBXVR<n>
   d. DBGWCR<n>
   e. DBGWVR<n>
   f. DBGWXVR<n>
   g. EDECCR
   h. EDITR
3. The SPR registers (for example, OSLSR_EL1.OSLK and EDSCR.TDA) and external pins are programmed to allow the following behavior:
   a. The execution of an **MSR** instruction in condition 1 to update its destination register without neither a system trap nor a debug halt
   b. The APB write operation in condition 2 to update its destination register without error
4. The **MSR** instruction execution in condition 1 and APB write operation in condition 2 happen in same

cycle.
5. The **MSR** write and the APB write are to two different registers. The architecture specifies that it is the software or debugger's responsibility to ensure writes to the same register are updated as expected.

Implications

If the above conditions are met, an execution of the **MSR** instruction might not update the destination register correctly. The destination register might contain one of following values after execution:

1. The execution of the **MSR** instruction is ignored. The destination register of the **MSR** instruction holds an old value.
2. The execution of the **MSR** instruction writes an incorrect value to its destination register.

A external debugger and system software are expected to be coordinated to prevent conflict in these registers.

Workaround

No workaround is required for this erratum.

2131905
Collision bit in PMBSR is reported incorrectly when there are multiple errors on SPE writes

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1. Fixed in r0p2.

Description

Collision information captured by PMBSR_EL1.COLL might be lost under certain circumstances, when the buffer management interrupt is raised.

Configurations Affected

This erratum affects all configurations.

Conditions

1. A sampling collision event is detected.
2. Subsequent SPE write results in 2 SEI errors.

Implications

If the above conditions are met, the collision indicator in PMBSR_EL1 is incorrectly set to 0, following the 2nd SEI error. PMBSR_EL1 does capture and set the "Data Loss" (DL) indicator and all the other PMBSR_EL1 fields correctly.

Workaround

There is no workaround for this erratum.

2132043
OSECCR_EL1/EDECCR is incorrectly included in the Warm Reset domain

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1. Fixed in r0p2.

Description

OSECCR_EL1/EDECCR is incorrectly included in the Warm Reset domain. If a Warm Reset occurs, then the value in this register will be lost.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Warm Reset is asserted.

Implications

If the above conditions are met, then the value in OSECCR_EL1/EDECCR will be lost.

Workaround

A debugger should enable a Reset Catch debug event by setting EDECR.RCE to 1. This causes the PE to generate a Reset Catch debug event on a Warm reset, allowing the debugger to reprogram the EDECCR.

2151898
A64 WFI or A64 WFE executed in Debug state suspends execution indefinitely

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2. Open.

Description

Executing an A64 WFI or WFE instruction while in Debug state results in suspension of execution, and execution cannot be resumed by the normal WFI or WFE wake-up events while in Debug state.

Configurations Affected

This erratum affects all configurations.

Conditions

1. The Processing Element (PE) is in Debug state and in AArch64 Execution state.
2. A WFI or WFE instruction is executed from EDITR.

Implications

If the above conditions are met, the PE will suspend execution.

This is not thought to be a serious erratum, because an attempt to execute a WFI or WFE instruction while in Debug state is not expected.

For WFI executed in Debug state, execution can only resume by any of the following:

- A Cold or Warm reset
- A Restart request trigger event from the Cross Trigger Interface (CTI) causing exit from Debug state, followed by a WFI wake-up event

For WFE executed in Debug state, execution can only resume by any of the following:

- A Cold or Warm reset
- A Restart request trigger event from the CTI causing exit from Debug state, followed by a WFE wake-up event
- An external event that sets the Event Register. Examples include executing an SEV instruction on another PE in the system or an event triggered by the Generic Timer.

Workaround

A workaround is unnecessary, because an attempt to execute a WFI or WFE instruction while in Debug state is not expected.

2242641
An SError might not be reported for an atomic store that encounters data poison

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

Under certain conditions, an atomic store that encounters data poison might not report an SError.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. An atomic store that is unaligned to its data size but within a 16-byte boundary accesses memory.
2. The atomic store accesses multiple L1 data banks such that not all banks have data poison.

Implications

If the above conditions are met, an SError might not be reported although poisoned data is consumed. Note that the data remains poisoned in the L1 and will be reported on the next access.

Workaround

This erratum has no workaround.

2280349
PMU L1D_CACHE_REFILL_OUTER is inaccurate

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

The L1D_CACHE_REFILL_OUTER PMU event 0x45 is inaccurate due to ignoring refills generated from a system cache. The L1D_CACHE_REFILL PMU event 0x3 should be the sum of PMU events L1D_CACHE_REFILL_INNER 0x44 and L1D_CACHE_REFILL_OUTER 0x45, however, due to the inaccuracy of L1D_CACHE_REFILL_OUTER 0x45 it is possible that this might not be the case.

Note: L1D_CACHE_REFILL PMU event 0x3 does accurately count all L1D cache refills, including refills from a system cache.

Configurations Affected

This erratum affects all configurations which implement a system cache.

Conditions

This erratum occurs under the following conditions:

1. The L2 inner cache is allocated with data transferred from a system cache.

Implications

When the previous condition is met, the L1D_CACHE_REFILL_OUTER PMU event 0x45 does not increment properly.

Workaround

The correct value of L1D_CACHE_REFILL_OUTER PMU event 0x45 can be calculated by subtracting the value of L1D_CACHE_REFILL_INNER PMU event 0x44 from L1D_CACHE_REFILL PMU event 0x3.

2296015
L1 Data poison is not cleared by a store

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2. Open.

Description

The L1 Data poison is not cleared by a store under certain conditions.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. A Processing Element (PE) executes a store that does not write a full word to a location that has data marked as poison.
2. The PE executes another store that writes to all bytes that contain data poison before the previous store is globally observable.

Implications

If the above conditions are met, then the poison bit in the L1 Data cache does not get cleared.

Workaround

This erratum can be avoided by inserting a DMB before and after a word-aligned store that is intended to clear the poison bit.

2341664
ESR_ELx.ISV can be set incorrectly for an external abort on translation table walk

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2. Open.

Description

When a data double bit error or external abort is encountered during a translation table walk, a synchronous exception is reported with the ISV bit set in the ESR_ELx register.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following condition:

1. A data double bit error or external abort is encountered during a translation table walk, and a synchronous exception is reported.

Implications

If the previous condition is met, the ESR_ELx.ISV bit will be set. The ESR[23:14] bits are set with the correct syndrome for the instruction making the access. That is SAS, SSE, SRT, SF, and AR are all set according to the instruction.

Workaround

This erratum has no workaround.

2346732
Lower priority exception might be reported when abort condition is detected at both stages of translation

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1 and r0p2. Open.

Description

When a permission fault or unsupported atomic fault is detected in the second stage of translation during stage 1 translation table walk, and there is a higher priority alignment fault due to SCTLR_EL1.C bit not being set, then Data Abort might be generated reflecting the lower priority fault.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs when all the following conditions apply:

1. The core executes an atomic, load/store exclusive, or load-acquire/store-release instruction.
2. SCTLR_EL1.C bit is not set and access is not aligned to size of data element.
3. A permission fault or unsupported atomic fault is detected in the second stage of translation during stage 1 translation table walk.

Implications

If the previous conditions are met, a Data Abort exception will be generated and incorrectly routed to EL2 with Data Fault Status Code (DFSC) of permission fault or unsupported atomic fault, when it should have been routed to EL1 with DFSC of alignment fault.

Workaround

This erratum has no workaround.

2423050
Software-step not done after exit from Debug state with an illegal value in DSPSR

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2. Open.

Description

On exit from Debug state, PSTATE.SS is set according to DSPSR.SS and DSPSR.M.
If DSPSR.M encodes an illegal value, then PSTATE.SS should be set according to the current Exception level. When the erratum occurs, the PE always writes PSTATE.SS to 0.

Configurations Affected

This erratum affects all configurations.

Conditions

- Software-step is enabled in current Exception level
- DSPSR.M encodes an illegal value, like:
  - M[4] set
  - M is a higher Exception level than current Exception level
  - M targets EL2 or EL1, when they are not available
- DSPSR.D is not set
- DSPSR.SS is set

Implications

If the previous conditions are met, then, on exit from Debug state the PE will directly take a Software-step Exception, without stepping an instruction as expected from DSPSR.SS=1.

Workaround

This erratum has no workaround.

2446530
PMU STALL_SLOT_BACKEND and STALL_SLOT_FRONTEND events count incorrectly

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

The following Performance Monitoring Unit (PMU) events do not count correctly:

- 0x3D, STALL_SLOT_BACKEND, no operation sent for execution on a slot due to the backend
- 0x3E, STALL_SLOT_FRONTEND, no operation sent for execution on a slot due to the frontend

Configurations Affected

This erratum affects all configurations.

Conditions

One of the PMU event counters is configured to count any of the following events:

- 0x3D, STALL_SLOT_BACKEND
- 0x3E, STALL_SLOT_FRONTEND

Implications

When operations are stalled in the processing element's dispatch pipeline slot, some of those slot stalls are counted as frontend stalls when they should have been counted as backend stalls, rendering PMU events 0x3D (STALL_SLOT_BACKEND) and 0x3E (STALL_SLOT_FRONTEND) inaccurate. The PMU event 0x3F (STALL_SLOT) does still accurately reflect its intended count of "No operation sent for execution on a slot".

Workaround

This erratum has no workaround.

2699192
Incorrect value reported for SPE PMU event SAMPLE_FEED

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

Under certain conditions when a CMP instruction is followed by a Branch, the SAMPLE_FEED PMU event 0x4001 is not reported.

Configurations Affected

This erratum affects all configurations.

Conditions

1. *Statistical Profiling Extension* (SPE) sampling is enabled.
2. SPE samples a CMP instruction, which is followed immediately by a BR instruction.

Implications

If the above conditions are met, then the SAMPLE_FEED event may not be incremented.

For most expected use cases, the inaccuracy is not expected to be significant.

Workaround

There is no workaround.

2699198
Reads of DISR_EL1 incorrectly return 0s while in Debug State

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

When the Processing Element (PE) is in Debug State, reads of DISR_EL1 from EL1 or EL2 with SCR_EL3.EA=0x1 will incorrectly return 0s.

Configurations Affected

This erratum affects all configurations.

Conditions

1. The PE is executing in Debug State at EL1 or EL2, with SCR_EL3.EA=0x1.
2. The PE executes an MRS to DISR_EL1.

Implications

If the above conditions are met, then the read of DISR_EL1 will incorrectly return 0s.

Workaround

No workaround is expected to be required.

2699762
Incorrect read value for Performance Monitors Control Register

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

The Performance Monitors Control Register (PMCR_EL0) and the External Performance Monitor Control Register (PMCR) might return an incorrect read value for the X field.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Software writes a nonzero value to the PMCR_EL0.X, or debugger writes a nonzero value to the PMCR.X
2. Software reads the PMCR_EL0 register, or debugger reads the PMCR register

Implications

The PMCR_EL1.X or PMCR.X field incorrectly reports the value 0x1, indicating exporting of events in an IMPLEMENTATION DEFINED PMU event export bus is enabled. The expected value is 0x0, as the implementation does not include a PMU event export bus.

Workaround

This erratum has no workaround.

2708634
DRPS instruction is not treated as UNDEFINED at EL0 in Debug state

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

In Debug state, DRPS is not treated as an UNDEFINED instruction.

Configurations Affected

This erratum affects all configurations.

Conditions

1. The *Processing Element* (PE) is in Debug state.
2. PE is executing at EL0.
3. PE executes DRPS instruction.

Implications

If the above conditions are met, then the PE will incorrectly execute DRPS as NOP instead of treating it as an UNDEFINFED instruction.

Workaround

There is no workaround.

2712565
Incorrect read value for Performance Monitors Configuration Register EX field

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

The Performance Monitors Configuration Register (PMCFGR) might return an incorrect read value for the EX field.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs when the software reads the PMCFGR register.

Implications

The PMCFGR.EX field incorrectly reports the value 0x1, indicating exporting of events in an IMPLEMENTATION DEFINED PMU event export bus is enabled. The expected value is 0x0, as the implementation does not include a PMU event export bus.

Workaround

This erratum has no workaround.

2764412
Incorrect value reported for SPE PMU event 0x4000 SAMPLE_POP

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

Under certain conditions the SAMPLE_POP PMU event 0x4000 might continue to count after SPE profiling has been disabled.

Configurations Affected

This erratum affects all configurations.

Conditions

1. *Statistical Profiling Extension* (SPE) sampling is enabled.
2. *Performance Monitoring Unit* (PMU) event counting is enabled.
3. SPE buffer is disabled, either directly by software, or indirectly via assertion of PMBIRQ, or by entry into Debug state.

Implications

If the previous conditions are met, then the SAMPLE_POP event might reflect an overcounted value. The impact of this erratum is expected to be very minor for actual use cases, as SPE sampling analysis is typically performed independently from PMU event counting.

Workaround

If a workaround is desired, then minimization of potential overcounting of the SAMPLE_POP event can be realized via software disable of any PMU SAMPLE_POP event counters whenever SPE is disabled, and also upon the servicing of a PMBIRQ interrupt. For profiling of EL0 workloads, software can further reduce exposure to overcounting by configuring the counter to not count at Exception levels of EL1 or higher.

2820248
PE might fail to detect multiple uncorrectable ECC errors in the L1 data cache tag RAM

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, and r0p2. Open.

Description

Under certain conditions, the *Processing Element* (PE) might fail to report multiple uncorrectable *Error Correction Code* (ECC) errors that occur in the L1 data cache tag RAM.

Configurations affected

This erratum affects all configurations.

Conditions

1. The PE detects and reports an uncorrectable ECC error in the L1 data cache tag RAM.
2. The PE detects a second uncorrectable ECC error in the L1 data cache tag RAM and an uncorrectable ECC error in the L1 data cache data RAM.

Implications

If the previous conditions are met, then the PE might fail to report the second uncorrectable ECC error in the L1 data cache tag RAM and the address recorded in ERR0ADDR might have an incorrect value. The ECC error occurring in the L1 data cache data RAM is reported correctly.

Workaround

No workaround is necessary. This erratum represents a condition where multiple uncorrectable ECC errors occur in a short period of time. While the PE does not report the errors correctly, ECC still provides a valuable mechanism for error detection and correction.