Arm Cortex-A520 Core (MP144)

Software Developer Errata Notice

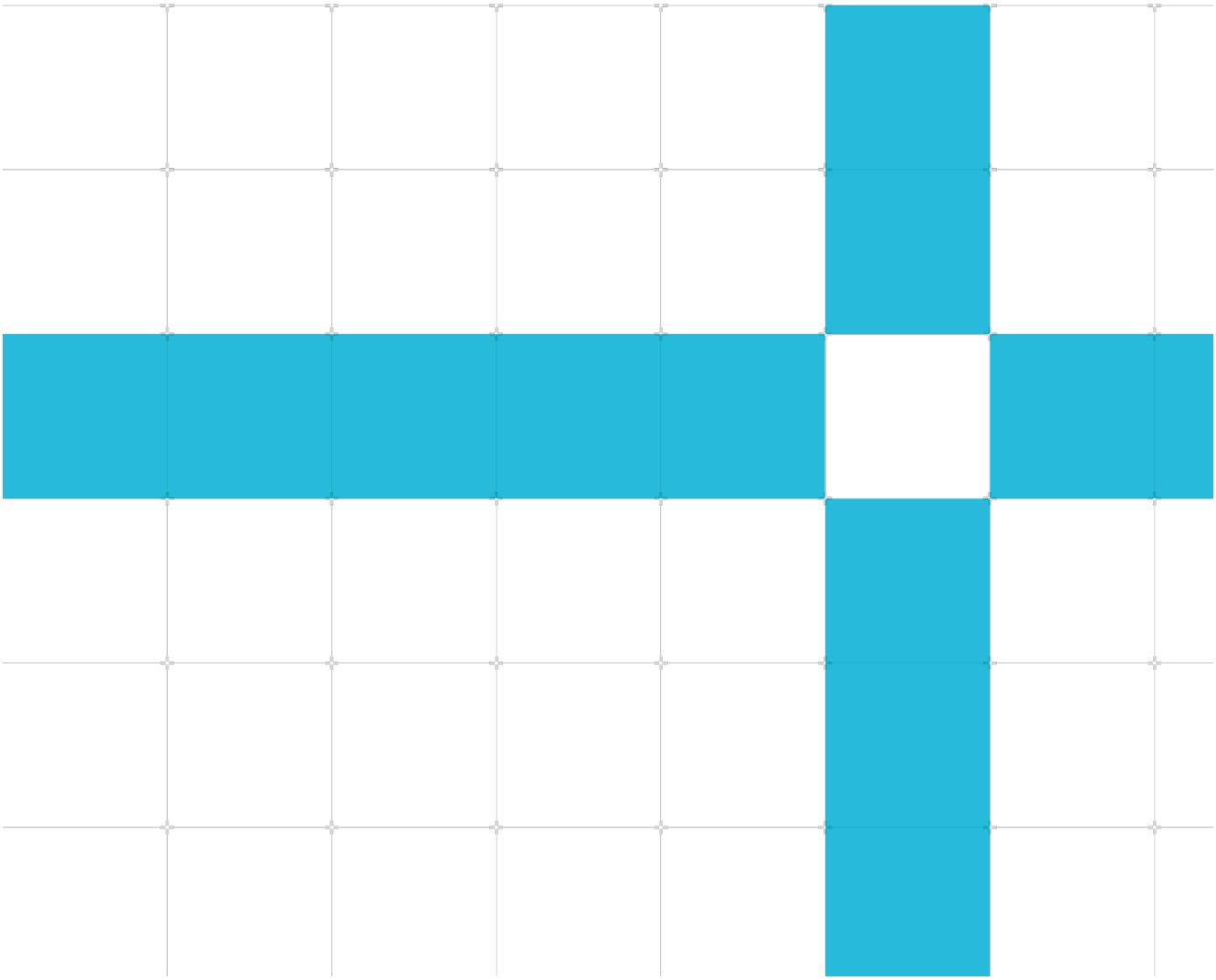
Date of issue: 08-Sep-2023

Non-Confidential

Document version: 5.0

Document ID: SDEN-2444153

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.

Feedback

Arm welcomes feedback on this product and its documentation. To provide feedback on Arm Cortex-A520 Core (MP144), 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.

08-Sep-2023: Changes in document version v5.0

ID	Status	Area	Category	Summary
2738620	Updated	Programmer	Category B	Deferred error might become uncontainable
2938996	New	Programmer	Category B	Data corruption might happen if TRBE is enabled
2966298	New	Programmer	Category B	A speculatively executed unprivileged load might leak data from a privileged via a cache side channel
2841875	New	Programmer	Category C	An uncontainable error might deadlock the cluster
2853709	New	Programmer	Category C	Error record registers indicate incorrect feature support in configurations without cache protection
2879977	New	Programmer	Category C	Unmodified cache line might be written back to memory
2940628	New	Programmer	Category C	Store data might be lost when a correctable error is detected in the L1 data cache
2969138	New	Programmer	Category C	Unmodified page table cache lines might be written back to memory

29-Mar-2023: Changes in document version v4.0

ID	Status	Area	Category	Summary
2858100	New	Programmer	Category B	Core may deadlock due to an ECC error in L1 data cache
2487790	Updated	Programmer	Category C	ERR0MISC1 value might be incorrect after multiple simultaneous errors detected
2751027	New	Programmer	Category C	Load operation might abort unexpectedly when accessing poisoned data
2803663	New	Programmer	Category C	Speculative dirty bit hardware update might happen for store operation
2833401	New	Programmer	Category C	Direct access to internal memory might not be reliable
2861633	New	Programmer	Category C	Some PMU events are incorrectly masked to trace unit
2871911	New	Programmer	Category C	LDG or MTE checked load/store might fail to detect poisoned data
2872870	New	Programmer	Category C	CE or DE errors from L1 data cache access might not be recorded in the RAS records

09-Dec-2022: Changes in document version v3.0

ID	Status	Area	Category	Summary
2630792	Updated	Programmer	Category B	Data corruption might occur during core powerdown
2738620	New	Programmer	Category B	Deferred error might become uncontainable
2710075	New	Programmer	Category C	Read value of IMP_CPUCFR_EL1 might be incorrect
2713358	New	Programmer	Category C	ERRxSTATUS.UET field might be incorrect
2713644	New	Programmer	Category C	Cache debug target for L2 Data RAM may not record correct data
2732181	New	Programmer	Category C	ERR2STATUS might be incorrect
2740664	New	Programmer	Category C	PMU event 0x77 CRYPTO_SPEC does not always count when enabled

29-Jul-2022: Changes in document version v2.0

ID	Status	Area	Category	Summary
2489489	New	Programmer	Category B	Atomic instructions might use older allocation tag for tag check
2630792	New	Programmer	Category B	Data corruption might occur during core powerdown
2655133	New	Programmer	Category B	Core might deadlock during transition from ON to OFF, or ON to OFF_EMU power mode
2658327	New	Programmer	Category B	BFMMLA instructions might produce incorrect result
2677201	New	Programmer	Category B	MTE check for store might not observe correct memory ordering
2680753	New	Programmer	Category B	A core might deadlock during powerdown if TRBE is enabled
2487790	New	Programmer	Category C	ERR0MISC1 value might be incorrect after multiple simultaneous errors detected
2572702	New	Programmer	Category C	ELADISABLE does not disable APB access to the complex ELA
2604637	New	Programmer	Category C	PMU event counts might be inaccurate
2626173	New	Programmer	Category C	ERR0STATUS.SERR might be incorrect
2626511	New	Programmer	Category C	Minimum power policy might prevent power off when FUNC_RET in use
2628441	New	Programmer	Category C	External aborts might result in a deadlock
2637415	New	Programmer	Category C	Core might not execute any instruction when performing Halting Step
2640950	New	Programmer	Category C	External 32-bit writes to some 64-bit RAS registers are not mapped correctly
2668978	New	Programmer	Category C	External aborts reporting cannot be disabled
2679529	New	Programmer	Category C	Multiple simultaneous errors report for L1 data cache might be incorrect
2681778	New	Programmer	Category C	TLBI not fully invalidating entries because of parity errors
2690489	New	Programmer	Category C	Some architectural PMU events are not always available to trace unit
2708967	New	Programmer	Category C	Read value of PMMIR is incorrect

08-Apr-2022: Changes in document version v1.0

ID	Status	Area	Category	Summary
2389819	New	Programmer	Category B	TLB not invalidated in complex power transitions
2441013	New	Programmer	Category B (rare)	Completion of affected memory accesses might not be guaranteed by completion of a TLBI
2567050	New	Programmer	Category C	Double-bit errors in the duplicate L1 data cache tag RAMs might lead to loss of coherency or deadlock

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
2389819	Programmer	Category B	TLB not invalidated in complex power transitions	r0p0	r0p1
2489489	Programmer	Category B	Atomic instructions might use older allocation tag for tag check	r0p0	r0p1
2630792	Programmer	Category B	Data corruption might occur during core powerdown	r0p0, r0p1	Open
2655133	Programmer	Category B	Core might deadlock during transition from ON to OFF, or ON to OFF_EMU power mode	r0p0	r0p1
2658327	Programmer	Category B	BFMMLA instructions might produce incorrect result	r0p0	r0p1
2677201	Programmer	Category B	MTE check for store might not observe correct memory ordering	r0p0	r0p1
2680753	Programmer	Category B	A core might deadlock during powerdown if TRBE is enabled	r0p0	r0p1
2738620	Programmer	Category B	Deferred error might become uncontainable	r0p0, r0p1	Open
2858100	Programmer	Category B	Core may deadlock due to an ECC error in L1 data cache	r0p0, r0p1	Open
2938996	Programmer	Category B	Data corruption might happen if TRBE is enabled	r0p0, r0p1	Open
2966298	Programmer	Category B	A speculatively executed unprivileged load might leak data from a privileged via a cache side channel	r0p0, r0p1	Open
2441013	Programmer	Category B (rare)	Completion of affected memory accesses might not be guaranteed by completion of a TLBI	r0p0	r0p1
2487790	Programmer	Category C	ERR0MISC1 value might be incorrect after multiple simultaneous errors detected	r0p0, r0p1	Open
2567050	Programmer	Category C	Double-bit errors in the duplicate L1 data cache tag RAMs might lead to loss of coherency or deadlock	r0p0	r0p1
2572702	Programmer	Category C	ELADISABLE does not disable APB access to the complex ELA	r0p0	r0p1
2604637	Programmer	Category C	PMU event counts might be inaccurate	r0p0	r0p1

ID	Area	Category	Summary	Found in versions	Fixed in version
2626173	Programmer	Category C	ERR0STATUS.SERR might be incorrect	r0p0	r0p1
2626511	Programmer	Category C	Minimum power policy might prevent power off when FUNC_RET in use	r0p0	r0p1
2628441	Programmer	Category C	External aborts might result in a deadlock	r0p0	r0p1
2637415	Programmer	Category C	Core might not execute any instruction when performing Halting Step	r0p0	r0p1
2640950	Programmer	Category C	External 32-bit writes to some 64-bit RAS registers are not mapped correctly	r0p0	r0p1
2668978	Programmer	Category C	External aborts reporting cannot be disabled	r0p0	r0p1
2679529	Programmer	Category C	Multiple simultaneous errors report for L1 data cache might be incorrect	r0p0	r0p1
2681778	Programmer	Category C	TLBI not fully invalidating entries because of parity errors	r0p0	r0p1
2690489	Programmer	Category C	Some architectural PMU events are not always available to trace unit	r0p0	r0p1
2708967	Programmer	Category C	Read value of PMMIR is incorrect	r0p0	r0p1
2710075	Programmer	Category C	Read value of IMP_CPUCFR_EL1 might be incorrect	r0p0, r0p1	Open
2713358	Programmer	Category C	ERRxSTATUS.UET field might be incorrect	r0p0, r0p1	Open
2713644	Programmer	Category C	Cache debug target for L2 Data RAM may not record correct data	r0p0, r0p1	Open
2732181	Programmer	Category C	ERR2STATUS might be incorrect	r0p0, r0p1	Open
2740664	Programmer	Category C	PMU event 0x77 CRYPTO_SPEC does not always count when enabled	r0p0, r0p1	Open
2751027	Programmer	Category C	Load operation might abort unexpectedly when accessing poisoned data	r0p0, r0p1	Open
2803663	Programmer	Category C	Speculative dirty bit hardware update might happen for store operation	r0p0, r0p1	Open
2833401	Programmer	Category C	Direct access to internal memory might not be reliable	r0p0, r0p1	Open
2841875	Programmer	Category C	An uncontainable error might deadlock the cluster	r0p0, r0p1	Open

ID	Area	Category	Summary	Found in versions	Fixed in version
2853709	Programmer	Category C	Error record registers indicate incorrect feature support in configurations without cache protection	r0p0, r0p1	Open
2861633	Programmer	Category C	Some PMU events are incorrectly masked to trace unit	r0p1	Open
2871911	Programmer	Category C	LDG or MTE checked load/store might fail to detect poisoned data	r0p0, r0p1	Open
2872870	Programmer	Category C	CE or DE errors from L1 data cache access might not be recorded in the RAS records	r0p0, r0p1	Open
2879977	Programmer	Category C	Unmodified cache line might be written back to memory	r0p0, r0p1	Open
2940628	Programmer	Category C	Store data might be lost when a correctable error is detected in the L1 data cache	r0p0, r0p1	Open
2969138	Programmer	Category C	Unmodified page table cache lines might be written back to memory	r0p0, r0p1	Open

Errata descriptions

Category A

There are no errata in this category.

Category A (rare)

There are no errata in this category.

Category B

2389819
TLB not invalidated in complex power transitions

Status

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

Description

If a core that is part of a complex powers on at the same time that the other core in the same complex is powering off, then the L2 *Translation Lookaside Buffer* (TLB) in the complex might not get invalidated correctly.

Configurations Affected

This erratum only affects configurations with two cores in a complex.

Conditions

1. One core in a complex is in the OFF power mode.
2. The other core in the same complex makes a transition from ON to OFF or OFF_EMU.
3. At the time the second core has almost completed its power transition, the first core starts a transition from OFF to ON.
4. A third core, outside the complex, executes a TLB invalidate instruction that would invalidate an entry that is currently held in the L2 TLB in the complex.

Implications

The L2 TLB in the complex is not invalidated by the power sequences, and so the core retains its previous state. However, there is a brief window in which the complex is disconnected from coherency with the rest of the system and so any TLB invalidate DVMs received during this time will not take effect. This can leave stale entries in the TLB that the cores in the complex might hit when they start executing code again.

Workaround

After a core is powered ON, the firmware should execute one of the following sequences before enabling the MMU, depending on whether the system expects to use Secure EL2 or not.

Without Secure EL2:

```
TLBI ALLE3
Set SCR_EL3.NS=0
ISB
TLBI ALLE1
Set SCR_EL3.NS=1
ISB
TLBI ALLE2
TLBI ALLE1
DSB SY
```

With Secure EL2:

```
TLBI ALLE3
Set SCR_EL3.NS=0
Set SCR_EL3.EEL2=1
ISB
TLBI ALLE2
TLBI ALLE1
Set SCR_EL3.NS=1
ISB
TLBI ALLE2
TLBI ALLE1
DSB SY
```

2489489
Atomic instructions might use older allocation tag for tag check

Status

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

Description

An atomic instruction might use an allocation tag that is no longer current for its tag check if relying on acquire/release-based ordering.

Configurations Affected

This erratum affects all configurations where the **BROADCASTMTE** pin is HIGH.

Conditions

The erratum occurs if the following conditions are met:

1. MTE checking is enabled.
2. The core executes an instruction with acquire semantics, other than an atomic instruction.
3. The core executes a tag-checked atomic instruction within 5 instructions of the instruction above, with no intervening `DMB`.
4. Timing-sensitive, microarchitectural conditions occur.

Implications

If the conditions are met, the tag read of the tag-checked atomic instruction might not be correctly ordered w.r.t. the preceding instruction with acquire semantics. This can result in a tag check using an allocation tag for the tag check that is no longer current, if another Processing Element has modified the allocation tag concurrently.

Workaround

This erratum can be avoided by the following instruction sequence:

```
MOVZ X1, #0x0000, LSL #0
MSR S3_6_C15_C4_0, X1

MOVK X1, #0x0000, LSL #0
MOVK X1, #0x0380, LSL #16
MOVK X1, #0x0000, LSL #32
MOVK X1, #0x0000, LSL #48
MSR S3_6_C15_C4_2, X1
```

```
MOVK X1, #0x0000, LSL #0
MOVK X1, #0x1FE0, LSL #16
MOVK X1, #0x0008, LSL #32
MOVK X1, #0x0000, LSL #48
MSR S3_6_C15_C4_3, X1

MOVK X1, #0x03F1, LSL #0
MOVK X1, #0x0110, LSL #16
MOVK X1, #0x0000, LSL #32
MOVK X1, #0x0000, LSL #48
MSR S3_6_C15_C4_1, X1

ISB
```

This is not expected to have a material performance impact in common use cases.

2630792
Data corruption might occur during core powerdown

Status

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

Description

Data corruption might occur when a core is powered down.

Configurations Affected

This erratum affects all configurations.

Conditions

The erratum occurs under the following conditions:

1. The core executes a PRFM PLDL1 or PRFM PSTL1 shortly before a WFI.
2. The core is requested to power off.
3. Timing sensitive microarchitectural conditions occur.

Implications

If the conditions are met, dirty data might be lost on the cache line accessed by the PRFM instructions, resulting in data corruption.

Workaround

To prevent this erratum from occurring, software can set IMP_CPUACTLR_EL1[38] = 1, for example, using the following sequence:

```
MRS x0, S3_0_C15_C1_0
MOV x1, #1
BFI x0, x1, #38, #1
MSR S3_0_C15_C1_0, x0
```

This might impact the effectiveness of some PRFM instructions. This is unlikely to have a measurable performance impact.

2655133
Core might deadlock during transition from ON to OFF, or ON to OFF_EMU power mode

Status

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

Description

The core might deadlock during a transition from ON to OFF, or ON to OFF_EMU power mode.

Configurations Affected

This erratum affects all configurations.

Conditions

The erratum occurs under the following conditions:

1. MMU is on
2. Hardware dirty bit update is enabled by SCTLR_ELx.HD or VTCR_EL2.HD
3. Core is transitioning from ON to OFF, or ON to OFF_EMU power mode
4. Timing sensitive microarchitectural conditions occur

Implications

If the previous conditions are met, the core might deadlock.

Workaround

To prevent this erratum from occurring during a transition from ON to OFF or ON to OFF_EMU power mode, the software must insert an ISB instruction before the WFI instruction.

2658327
BFMMLA instructions might produce incorrect result

Status

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

Description

When both cores in a complex are executing chained multiply-accumulate instructions, then under precise timing conditions a **`BFMMLA`** instruction might produce an incorrect result.

Configurations Affected

This erratum affects any configuration with 2 cores in a complex, sharing a 2x64-bit VPU datapath (configuration parameter VPU_DATAPATH is set to 2x64). Configurations sharing a 2x128-bit datapath are unaffected. Affected configurations can be identified by reading IMP_CPUCFR_EL1 using **`MRS Xt, S3_0_C15_C0_0`** - the core is affected if bit [16] is 1 and bit [4] is 0.

Conditions

This erratum occurs under the following conditions:

1. Both cores in the complex are executing chained multiply-accumulate instructions.
2. One core in the complex flushes a chained multiply-accumulate instruction executed speculatively.
3. A **`BFMMLA`** or multicycle vector instruction is executed after the flush.
4. Precise microarchitectural timing conditions occur.

Any of the following instructions are classed as chained multiply-accumulate instructions:

- **`BFMMLA`**
- **`BFDOT`**

Any of the following instructions are classed as multicycle vector instructions:

- **`FDIV*`**
- **`FSQRT`**
- **`SDIV*/UDIV*`**
- **`BDEP/BEXT/BGRP`**
- **`PMULL*`**
- **`RAX1`**
- **`SHA512*`**

- **SM3*/SM4E***

Implications

If these conditions are met, the result of a **BFMMLA** executed by either core might be incorrect. As FEAT_BF16 is a recent addition to the architecture, these instructions are not expected to be present in legacy code.

Workaround

There is no complete workaround for this erratum. It is expected that software will use run-time feature detection to determine whether to use these instructions or to fall back on support for earlier architecture versions. A kernel can avoid this erratum by updating the detected feature list to remove FEAT_BF16 from the list of supported features in affected systems.

2677201
MTE check for store might not observe correct memory ordering

Status

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

Description

Memory Tagging Extension (MTE) check on a store might not be correctly ordered with respect to an earlier DMB or instruction with acquire semantics.

Configurations Affected

This erratum affects configurations with BROADCASTMTE=true.

Conditions

This erratum occurs under the following conditions:

1. MTE checking is enabled, by setting (SCTLR_ELx.ATAn = 1, SCTLR_ELx.TCFn != 0b00).
2. The core executes an instruction with acquire semantics, or a DMBLD/DMBSY.
3. A checked store instruction is executed to Inner Writeback and Outer Writeback, tagged, memory.
4. Timing-sensitive, micro-architecural conditions occur.

Implications

If the conditions are met, the MTE check on the store might not be correctly ordered w.r.t. the DMB or instruction with acquire semantics. This might result in an incorrect update of the TFSR_ELx register, or MTE check abort wrongly generated or missed to generate.

Workaround

To prevent this erratum from occurring for DMB operation, software can set IMP_CPUACTLR_EL1[10] = 1, for example, using the following sequence:

```
MRS x0, S3_0_C15_C1_0
MOV x1, #1
BFI x0, x1, #10, #1
MSR S3_0_C15_C1_0, x0
```

To prevent this erratum from occurring for Load Acquire operation, software can use the following instruction sequence

```
MOVZ X1, #0x0000, LSL #1
MSR S3_6_C15_C4_0, X1

MOVK X1, #0x0000, LSL #0
MOVK X1, #0x0850, LSL #16
MOVK X1, #0x0000, LSL #32
MOVK X1, #0x0000, LSL #48
MSR S3_6_C15_C4_2, X1

MOVK X1, #0x0000, LSL #0
MOVK X1, #0x1F70, LSL #16
MOVK X1, #0x0008, LSL #32
MOVK X1, #0x0000, LSL #48
MSR S3_6_C15_C4_3, X1

MOVK X1, #0x03F1, LSL #0
MOVK X1, #0x00C0, LSL #16
MOVK X1, #0x0000, LSL #32
MOVK X1, #0x0000, LSL #48
MSR S3_6_C15_C4_1, X1
ISB
```

2680753
A core might deadlock during powerdown if TRBE is enabled

Status

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

Description

A core might deadlock during powerdown if *TRace Buffer Extension* (TRBE) is enabled.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. The TRBE is enabled by setting TRBLIMITR_EL1.E = 0b1. The core is executing in a non-prohibited trace region.
2. The core executes a WFI, WFIT, WFE or WFET instuction.
3. An external wakeup or timeout occurs, waking up the core.
4. The core executes a WFI instruction to power down the core.
5. system rely on the core to be ready to enter to power OFF/OFF_EMU state
6. Timing-sensitive micro-architectural conditions occur.

Implications

If the conditions are met, the core might not accept the power state transition to OFF/OFF_EMU state and system may deadlock.

Workaround

Software can execute a **`TSB CSYNC`** and **`DSB before execute WFI for power down`**.

2738620
Deferred error might become uncontainable

Status

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

Description

Poison information cached in a *Processing Element* (PE) might be lost and therefore make the deferred error to become uncontainable.

Configurations affected

This erratum affects configurations having parameter CORE_CACHE_PROTECTION set to TRUE and any of the following:

1. The parameter BROADCASTMTE is set to TRUE.
2. The interconnect does not have a precise snoop filter, and does not use SnpQuery to inquire about the state of the line at the *Request Node* (RN).

Conditions

This erratum might occur if line A (Normal Inner Write-Back, Outer Write-Back Cacheable) is cached in the PE and another cache in the system, one cache has the line as poisoned, and one of the following conditions is met:

1. A MakeReadUnique from the complex is processed by the interconnect and poisoned data is returned, without the line being lost by the complex.
2. The non-L1 allocating store operation executed by this PE and the store operation modifies less than a cache line worth of MTE tags.

Implications

If the condition occurs, the line might be propagated to the core without being poisoned.

Workaround

Software can enable the Error Recovery Interrupt for deferred error by setting the DUI bit of all the *Reliability, Availability, and Serviceability* (RAS) node registers ERRxCTLR, and treat all deferred errors as uncontainable.

2858100
Core may deadlock due to an ECC error in L1 data cache

Status

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

Description

A deadlock might occur as a result of a load accessing a L1 data cache line which has ECC error.

Configurations Affected

This erratum affects configurations with CPU_CACHE_PROTECTION set.

Conditions

The erratum occurs under the following conditions:

1. A load or store sees an ECC error or deferred error in the L1 data cache.
2. Very unlikely, timing sensitive microarchitectural conditions occur.

Implications

If the above conditions are met, the core might deadlock. The core will continue normal operation if any coherency operation is seen.

Workaround

There is still substantial benefit being gained from the ECC logic. There might be a small increase in overall system failure rate due to this erratum.
To prevent this erratum from occurring, software can set IMP_CPUACTLR_EL1[29] = 1, for example, using the following sequence:

```
MRS x0, S3_0_C15_C1_0
MOV x1, #1
BFI x0, x1, #29, #1
MSR S3_0_C15_C1_0, x0
```

This will reduce the effectiveness of internal clock gating, and might impact power efficiency. During power testing of sample silicon, Arm recommends not applying the workaround.

2938996
Data corruption might happen if TRBE is enabled

Status

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

Description

Data might be corrupted if *TRace Buffer Extension* (TRBE) is enabled.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. The TRBE is enabled by setting TRBLIMITR_EL1.E = 0b1.
2. The trace data store to the memory cross 4k page.
3. One of the 4k page has translation fault or permission fault.
4. Timing-sensitive micro-architectural conditions occur.

Implications

If the above conditions are met, random data might be corrupted before the core takes the TRBE IRQ.

Workaround

The EL3 firmware can prevent trace collection via TRBE by programming MDCR_EL3.NSTB[1] to the opposite value of SCR_EL3.NS on a security state switch.

2966298
A speculatively executed unprivileged load might leak data from a privileged via a cache side channel

Status

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

Description

A speculatively executed unprivileged load might leak data from a privileged via a cache side channel.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. A load is speculatively executed at EL0, accessing a location in memory that is mapped, but lacks EL0 access permissions.
2. Timing-sensitive, microarchitectural conditions occur.

Implications

The speculatively executed load can, under specific microarchitectural conditions, speculatively forward data, bypassing a permission check, to the address operand of another load, potentially leaking information from a higher privilege level via a cache side channel. Leakage via other side channels, or involving forwarding via ALU operations before forwarding to a load instruction is not possible.

Pagetable isolation between EL0 and higher level ELs prevents the issue from occurring.

Workaround

If pagetable isolation is disabled, the context switch logic in the kernel can be updated to execute the following sequence on affected cores before exiting to EL0, and after all explicit memory accesses:

1. A non-shareable TLBI to any context and/or address, including unused contexts or addresses, such as a `TLBI VALE1 Xzr`.
2. A DSB NSH to guarantee completion of the TLBI.

Category B (rare)

2441013
Completion of affected memory accesses might not be guaranteed by completion of a TLBI

Status

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

Description

The core might not guarantee completion of all memory accesses after completion of a TLB Invalidate (`TLBI`) instruction affecting those accesses on another core.

Configurations affected

This erratum affects all configurations.

Conditions

1. Another PE in the system executes a `TLBI` or Instruction Cache (`IC`) instruction, followed by a Data Synchronization Barrier (`DSB`) instruction.
2. The core executes a store to a memory location A.
3. Another PE in the system modifies the descriptor used by the store to memory location A, using a break-before-make sequence.
    - The break-before-make sequence will include a `TLBI` instruction, followed by a `DSB` instruction.
4. Rare, timing-sensitive, microarchitectural conditions occur.

Implications

The `DSB` used after the `TLBI` as part of the break-before-make sequence might not guarantee the completion of the store to memory location A under very rare and unlikely timing conditions. For most systems and applications, the latency of the break-before-make sequence and time until later reuse is very likely to exceed the latency required to naturally complete the store.

Workaround

Given the rarity of the conditions needed to trigger this erratum, a workaround is not expected to be needed in most systems.
If a workaround is required, then the **TLBI**, **DSB** sequence from the break-before-make sequence can be repeated. After repeating the **TLBI**, **DSB** sequence, all memory accesses that use a translation changed by the break-before-make sequence will have completed.

Category C

2487790
ERR0MISC1 value might be incorrect after multiple simultaneous errors detected

Status

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

Description

If multiple *Error Correcting Code* (ECC) errors are simultaneously detected in the L1 data cache, the reported ERR0MISC1.Bank value and/or ERR0MISC1.Granule field value for the L1 data cache MTE data RAMs might be incorrect.

Configurations Affected

This erratum affects configurations where the CORE_CACHE_PROTECTION parameter is TRUE.

Conditions

This erratum occurs under the following conditions:

1. ECC errors are detected in multiple banks in the same cycle in either the L1 data cache data RAMs or the L1 data cache MTE data RAMs.
2. At least one of the errors is of a higher severity than one of the others.

Implications

There is still substantial benefit being gained from the ECC logic. There might be a negligible increase in overall system failure rate due to this erratum.

If the conditions are met, the value reported in the ERR0MISC1.Bank and/or ERR0MISC1.Granule field in the core RAS register block might be incorrect, and report the RAM bank/granule of the error in the lowest-numbered bank/granule rather than the bank/granule of the highest-priority error. The Array, Entry, SubBank fields will be correct (these field values are the same for all the simultaneously detected errors). The ERR0STATUS and ERR0MISC0 registers will correctly report the highest-priority error, and the ERR0MISC1.Granule is still correct for L1 data cache data RAM.

Workaround

No workaround is required.

2567050
Double-bit errors in the duplicate L1 data cache tag RAMs might lead to loss of coherency or deadlock

Status

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

Description

If a double-bit error is detected on a read of the duplicate L1 data cache tag RAMs, a deadlock might occur.

Configurations Affected

This erratum affects configurations with core cache protection enabled.

Conditions

The erratum can occur under two sets of conditions.

Set 1:

1. A `DC ISW`, `DC CSW`, or `DC CISW` operation to the L1 data cache is executed. No error is detected on the read of the duplicate L1 data cache tag RAMs.
2. The same core performs an L1 data cache refill for a line in the same set as the set/way operation above. This refill might be speculative.
3. A double-bit error occurs on a read of the duplicate L1 data cache tag RAMs for the L1 cache refill above.

Set 2:

1. A new or deferred error is detected in the L1 data cache tag, data, dirty, or Memory Tagging Extension (MTE) RAMs. This causes a hardware set/way operation being generated.
2. For the hardware-initiated set/way maintenance operation above, no error is detected on the read of the duplicate L1 data cache tag RAMs.
3. The same core performs an L1 data cache refill for a line in the same set as the set/way operation above. This refill might be speculative.
4. A double-bit error occurs on a read of the duplicate L1 data cache tag RAMs for the L1 data cache refill above.

Implications

There is still substantial benefit being gained from the ECC logic. There might be a negligible increase in overall system failure rate due to this erratum. If the conditions are met, coherency might be lost or a deadlock might occur on later memory accesses. Double-bit errors on the duplicate L1 data cache tag RAMs are classed as uncontainable, and Arm believes these implications are in line with those of an uncontainable error. The detection and reporting of the error are unaffected.

Workaround

The first set of conditions can be avoided by software. The use of data cache maintenance by set/way operations to the L1 data cache is not necessary as the core performs automatic cache maintenance on powerup and powerdown. Where software intends to use set/way operations regardless, the data cache should be turned off to ensure the intended behavior of cleaning the cache and avoiding a speculative refill to the cache during the sequence.

The second set of conditions does not have a workaround. However, a double-bit error occurring in the duplicate tag RAMs on a cache line that has previously had another error in the L1 data cache is very unlikely.

2572702
ELADISABLE does not disable APB access to the complex ELA

Status

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

Description

ELADISABLE is a cluster configuration signal. When it is HIGH, it disables access to all ELAs in the cluster. Due to this erratum, if an ELA is configured in the complex, it is still accessible through the debug APB interface when ELADISABLE is HIGH. The ROM table entry for the complex ELA will still be removed, so it is not discoverable by an external debugger.

Configurations Affected

All configurations with the complex ELA are affected.

Conditions

The erratum occurs if all the following conditions apply:

1. ELADISABLE is HIGH
2. A Debug APB access is made to the memory-mapped region for the complex ELA

Implications

This erratum means that the complex ELA cannot be completely disabled. Assuming the correct address offset is already known, a debugger will have free control of the trigger and trace features. The ELA can also stop the core clock, which is its only invasive debug feature. This can still be disabled through the authentication interface (DBGEN and SPIDEN), but this also disables all other invasive debug features in the cluster.

Workaround

This erratum has no workaround.

2604637
PMU event counts might be inaccurate

Status

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

Description

The following performance events might be unreliable due to this erratum:

- 0x811D BR_IND_RETIRED
- 0x8116 BR_INDNR_PRED_RETIRED
- 0x8117 BR_INDNR_MIS_PRED_RETIRED
- 0x810C BR_INDNR_TAKEN_RETIRED
- 0x8110 BR_IMMED_PRED_RETIRED
- 0x8111 BR_IMMED_MIS_PRED_RETIRED
- 0x811C BR_PRED_RETIRED
- 0x8114 BR_RETURN_PRED_RETIRED
- 0x8115 BR_RETURN_MIS_PRED_RETIRED
- 0x0019 BUS_ACCESS
- 0x0061 BUS_ACCESS_WR
- 0x818D BUS_REQ_RD
- 0x8125 BUS_REQ_RD_PERCYC
- 0x8128 DTLB_WALK_PERCYC
- 0x8129 ITLB_WALK_PERCYC
- 0x0040 L1D_CACHE_RD
- 0x0041 L1D_CACHE_WR
- 0x00C4 L1D_WS_MODE_ENTRY
- 0x0016 L2D_CACHE
- 0x0020 L2D_CACHE_ALLOCATE
- 0x8155 L2D_CACHE_HWPRF
- 0x81BD L2D_CACHE_REFILL_HWPRF
- 0x0018 L2D_CACHE_WB
- 0x0051 L2D_CACHE_WR
- 0x002B L3D_CACHE
- 0x400B L3D_CACHE_LMISS_RD
- 0x4021 LD_ALIGN_LAT
- 0x0072 LDST_SPEC
- 0x4020 LDST_ALIGN_LAT
- 0x4024 MEM_ACCESS_CHECKED
- 0x4025 MEM_ACCESS_RD_CHECKED
- 0x4026 MEM_ACCESS_WR_CHECKED
- 0x8121 MEM_ACCESS_RD_PERCYC
- 0x4022 ST_ALIGN_LAT

- 0x0024 STALL_BACKEND
- 0x8165 STALL_BACKEND_L1D

Configurations Affected

- For the STALL_BACKEND_L1D event, this erratum affects all configurations with L2 cache.
- For the other events, this erratum affects all configurations.

Conditions

No specific conditions are needed.

Implications

The affected events have been divided into categories:

- Events in the Low impact category still produce an indicative result in most cases.
- Events in the High impact category are too inaccurate to be used, unless they have a workaround.

Low impact:

- The L2D_CACHE_WB, L2D_CACHE, L2D_CACHE_HWPRF and L2D_CACHE_REFILL_HWPRF events might overcount if a request sees a protocol-level retry. Protocol-level retries between the core and the DSU are not common.
- The STALL_BACKEND event might slightly undercount. The STALL_BACKEND_L1D event might slightly overcount.
- The L3D_CACHE, L2D_CACHE_WR, and L2D_CACHE_ALLOCATE events might undercount.
- The LDST_SPEC event might undercount. The sum of LD_SPEC and ST_SPEC events gives the expected result.
- Long latency misses might cause L1D_CACHE_RD, L1D_CACHE_WR, and L1D_WS_MODE_ENTRY events to overcount.
- Long latency misses might cause STALL_BACKEND_L2D event to undercount.

High impact, with complete workaround:

- The affected BR events can overcount or undercount significantly depending on whether other BR events are enabled or not. The affected events will count accurately if all of the following are also enabled: PC_WRITE_RETIRED, BR_RETIRED, BR_IMMED_RETIRED, BR_RETURN_RETIRED, BR_MIS_PRED_RETIRED.
- LD_ALIGN_LAT, ST_ALIGN_LAT, LDST_ALIGN_LAT, and the affected MEM_ACCESS* events will not count at all unless an event number in the range 0 to 0x1FF is also enabled. Otherwise, they are accurate.

- L3D_CACHE_LMISS_RD might undercount significantly. 0x00A2 L3D_CACHE_REFILL_RD can be used instead as a workaround.

High impact, with approximate or no workaround:

- The BUS_REQ_RD event might significantly overcount. If the number of Inner-Writeback and Outer-Writeback cacheable accesses far exceeds non-cached accesses, BUS_REQ_RD event can instead be approximated by BUS_ACCESS_RD/2.
- The BUS_ACCESS and BUS_ACCESS_WR events are not accurate.
- The count of *PERCYC events can appear to overflow at multiples of 256, making their counts much smaller than expected.

Workaround

Some of the affected events have workarounds, which are mentioned in the implications section.

For the remaining events, there are no workarounds.

2626173
ERR0STATUS.SERR might be incorrect

Status

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

Description

The SERR field of the ERR0STATUS register might be updated incorrectly.

Configurations Affected

This erratum affects all configurations.

Conditions

The erratum occurs under the following conditions:

1. The core executes an SVE non-fault, first-fault or predicated load instruction.
2. The core executes another load instruction, and this load follows the load above with a maximum of one other instruction in between.
3. Both of these two instructions see an external abort (NDerr or Derr) or poison data. The abort must be different between the two.
4. Timing-sensitive, micro-architectural conditions occur.

Implications

There is still substantial benefit being gained from the *Error Correction Code* (ECC) logic. There might be a negligible increase in overall system failure rate due to this erratum.
If the conditions are met, the RAS ERR0STATUS.SERR field might be set to 18 instead of the expected values of 12 or 21.

Workaround

No workaround is required.

2626511
Minimum power policy might prevent power off when FUNC_RET in use

Status

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

Description

The core supports putting the VPU logic in a low power state with the FUNC_RET power mode. If the power mode is in use while the PPU minimum power policy mode is also set to the FULL_RET or FUNC_RET, then it can prevent the other core in the same complex from powering off.

Configurations Affected

This erratum affects all configurations with two cores in a complex.

Conditions

1. One core in the complex has the IMP_CPUPWRCTLR_EL1.VPU_PWR_CTLR register set to a nonzero value.
2. The core does not execute any instructions that use the VPU for a period and therefore enters the FUNC_RET power mode.
3. The IMP_CPUPWRCTLR_EL1.CORE_PWRDN_EN bit is set. This might happen before or after condition 2.
4. The core executes a WFI instruction.
5. The PPU for that core is in dynamic mode with the minimum power policy programmed to FULL_RET or FUNC_RET in the PPU_PWPR.PWR_POLICY field.
6. The other core in the complex requests a power transition from ON to OFF, ON to OFF_EMU, or OFF_EMU to OFF.

Implications

If the erratum occurs, the second core in the complex will not be able to complete its power transition until the first core has moved from FUNC_RET to ON. However, the first core will not be correctly indicating to the PPU that it needs to transition to ON, therefore, neither core will be able to proceed, which could lead to a system deadlock. If during this time the minimum power mode of the first core is changed to OFF or OFF_EMU then the first core will transition to that power mode, which will then allow the second to complete its transition.

Arm does not expect the minimum power policy to typically be set to FUNC_RET or FULL_RET if the core is going to want to power off, because that would prevent the core from powering off.

Workaround

For systems that never set the core's minimum power policy to FULL_RET or FUNC_RET, no workaround is necessary. If a workaround is required, then as part of the powerdown sequence, EL3 software should set the IMP_CPUPWRCTLR_EL1.VPU_PWR_CTLR field to zero before it sets the IMP_CPUPWRCTLR_EL1.CORE_PWRDN_EN field.

2628441
External aborts might result in a deadlock

Status

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

Description

A deadlock might occur as a result of a load accessing a cache line with an external abort.

Configurations Affected

This erratum affects all configurations.

Conditions

The erratum occurs under the following conditions:

1. A load accesses a cache line that sees an external abort.
2. Timing sensitive conditions occur.

Implications

There is still substantial benefit being gained from the *Error Correcting Codes* (ECC) logic. There might be a negligible increase in overall system failure rate due to this erratum. If the conditions are met, the load might deadlock.

Workaround

There is still substantial benefit being gained from the ECC logic. There might be a small increase in overall system failure rate due to this erratum.

To prevent this erratum from occurring during functional testing, software can set IMP_CPUACTLR_EL1[29] = 1, for example, using the following sequence:

```
MRS x0, S3_0_C15_C1_0
MOV x1, #1
BFI x0, x1, #29, #1
MSR S3_0_C15_C1_0, x0
```

This will reduce the effectiveness of internal clock gating, and might impact power efficiency. During power testing of sample silicon, Arm recommends not applying the workaround.

2637415
Core might not execute any instruction when performing Halting Step

Status

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

Description

Halting Step is a debug resource that a debugger can use to make the core step through code one instruction at a time. Due to this erratum, the core might not execute any instruction before returning to debug state.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs when the following conditions are true for the sequence described below:

- DBGEN == 1.
- SPIDEN == 0.
- Halting Step is enabled by EDECR.SS.

Then the following sequence must occur:

1. The core exits Debug State to Non-secure state.
2. The core must execute **`ESB`** instruction with a physical SError pending and unmasked according to the table in the "Asynchronous exception masking" section of the Arm Architecture Reference Manual Armv8, for A-profile architecture. The SError must generate an exception targeting EL3.
3. The core performs an ERET from EL3 to a Non-secure state.
4. The core starts executing an instruction that will not get an exception targeting EL3.

Implications

The instruction at step 4 of the above sequence should be executed, then the core should enter debug state. Instead, the core will enter debug state without executing that instruction.

The next time the core attempt to step that instruction, it will be executed, and then the core will enter debug state in the correct manner.

Workaround

This erratum has no workaround.

2640950
External 32-bit writes to some 64-bit RAS registers are not mapped correctly

Status

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

Description

Writing to the upper or lower 32 bits of a 64-bit RAS register is permitted. Due to this erratum, some addresses are mapped to the incorrect range of bits inside a register.

In the core node, writes addressed to the upper 32 bits of the following registers update the lower 32 bits instead. The upper 32 bits are inaccessible by 32-bit writes.

- ERR0MISC0_EL1
- ERR0MISC1_EL1

The same issue applies to the following core node registers, but their upper 32 bits are RES0, so 32-bit writes to those addresses are not expected.

- ERR0CTLR_EL1
- ERR0PFGCDN_EL1
- ERR0PFGCTL_EL1
- ERR0STATUS_EL1

In the Complex node, writes addressed to the upper 32 bits of ERR0MISC1_EL1 update the lower 32 bits instead. Also, writes addressed to the lower 32 bits update the upper 32 bits instead.

Configurations Affected

All configurations are affected.

Conditions

This erratum occurs whenever there is a 32-bit external write to the upper 32 bits of the affected registers.

Implications

For the affected registers which contain error record information, it is not possible to clear them completely using only 32-bit external writes.
For the affected registers which control error records or pseudo-fault generation, the settings in the lower 32 bits can be corrupted.
All affected registers can still be read as expected using 32-bit reads from the assigned addresses.

Workaround

This erratum can be avoided by using 64-bit writes for the affected registers.

2668978
External aborts reporting cannot be disabled

Status

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

Description

A system able to generate External aborts or poison might see errors reported by the L2 node, even if error reporting is disabled.

Configurations Affected

This erratum affects configurations with CORE_CACHE_PROTECTION enabled (CORE_CACHE_PROTECTION set to 1).

Conditions

- ERR0CTRL.ED is set to 0b0
- Data or responses are received by the core with Data Error, Non-data Error, or poison

Implications

If the previous conditions are met, an error might be reported.
Interrupts generated by the set of conditions can be masked by clearing ERR0CTLR.FI and ERR0CTLR.UI.

Workaround

This erratum has no workaround.

2679529
Multiple simultaneous errors report for L1 data cache might be incorrect

Status

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

Description

If multiple *Error Correcting Code* (ECC) errors are simultaneously detected in the L1 data cache, the reported ERR0MISC0 and ERR0STATUS for the L1 data cache Data RAM or *Memory Tagging Extension* (MTE) data RAMs might be incorrect.

Configurations Affected

This erratum affects configurations where the CORE_CACHE_PROTECTION parameter is TRUE.

Conditions

This erratum occurs under the following conditions:

1. ECC errors are detected in multiple banks in the same cycle in either the L1 data cache data RAMs or the L1 data cache MTE data RAMs.
2. The ECC error happen in different index/way.

Implications

There is still substantial benefit being gained from the ECC logic. There might be a negligible increase in overall system failure rate due to this erratum.

If the conditions are met, the value reported in the ERR0STATUS, ERR0MISC0.INDX and/or ERR0MISC0.WAY field in the core RAS register block might be incorrect. It can be either:

- The ERRSTATUS may not report the highest priority error of the simultaneous error for Data RAM, but the index/way information report is still correspond to the report error
- The ERRSTATUS report the highest priority error of the simultaneous error for MTE data RAM, but the index/way information may not corresponding to the highest priority error for the MTE data RAM.

Workaround

No workaround is required for this erratum.

2681778
TLBI not fully invalidating entries because of parity errors

Status

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

Description

Entries might not be fully invalidated on TLBI because of parity errors.

Configurations Affected

This erratum affects all configurations.

Conditions

The erratum occurs under the following conditions:

- The Complex receives a DVM TLBI.
- TLB prefetches are enabled.
- Parity errors occurring.
- Uncommon, timing-sensitive micro-architectural conditions occur.

Implications

If the previous conditions are met, a TLBI might not invalidate some entries in the TLB.
There is still substantial benefit being gained from the ECC logic. There might be a negligible increase in overall system failure rate due to this erratum.

Workaround

No workaround is expected to be required for engineering samples.

2690489
Some architectural PMU events are not always available to trace unit

Status

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

Description

The PMU architectural events are available to the trace unit through the extended input facility. Due to this erratum, some architectural events might not be sent to the trace unit after being selected. The affected events include most events above 0x4000:

- 0x4005 STALL_BACKEND_MEM
- 0x4006 L1I_CACHE_LMISS
- 0x4009 L2D_CACHE_LMISS_RD
- 0x400B L3D_CACHE_LMISS_RD
- 0x4020 LDST_ALIGN_LAT
- 0x4021 LD_ALIGN_LAT
- 0x4022 ST_ALIGN_LAT
- 0x4024 MEM_ACCESS_CHECKED
- 0x4025 MEM_ACCESS_CHECKED_RD
- 0x4026 MEM_ACCESS_CHECKED_WR
- 0x8002 SVE_INST_RETIRED
- 0x8006 SVE_INST_SPEC
- 0x8014 FP_HP_SPEC
- 0x8018 FP_SP_SPEC
- 0x801C FP_DP_SPEC
- 0x80E3 ASE_SVE_INT8_SPEC
- 0x80E7 ASE_SVE_INT16_SPEC
- 0x80EB ASE_SVE_INT32_SPEC
- 0x80EF ASE_SVE_INT64_SPEC
- 0x810C BR_INDNR_TAKEN_RETIRED
- 0x8110 BR_IMMED_PRED_RETIRED
- 0x8111 BR_IMMED_MIS_PRED_RETIRED
- 0x8114 BR_RETURN_PRED_RETIRED
- 0x8115 BR_RETURN_MIS_PRED_RETIRED
- 0x8116 BR_INDNR_PRED_RETIRED
- 0x8117 BR_INDNR_MIS_PRED_RETIRED
- 0x811C BR_PRED_RETIRED
- 0x811D BR_IND_RETIRED
- 0x8120 INST_FETCH_PERCYC
- 0x8121 MEM_ACCESS_RD_PERCYC
- 0x8124 INST_FETCH
- 0x8125 BUS_REQ_RD_PERCYC

- 0x8128 DTLB_WALK_PERCYC
- 0x8129 ITLB_WALK_PERCYC
- 0x8134 DTLB_HWUPD
- 0x8135 ITLB_HWUPD
- 0x8136 DTLB_STEP
- 0x8137 ITLB_STEP
- 0x8138 DTLB_WALK_LARGE
- 0x8139 ITLB_WALK_LARGE
- 0x813A DTLB_WALK_SMALL
- 0x813B ITLB_WALK_SMALL
- 0x813C DTLB_WALK_RW
- 0x8145 L1I_CACHE_HWPRF
- 0x8154 L1D_CACHE_HWPRF
- 0x8155 L2D_CACHE_HWPRF
- 0x8156 L3D_CACHE_HWPRF
- 0x8158 STALL_FRONTEND_MEMBOUND
- 0x8159 STALL_FRONTEND_L1I
- 0x815B STALL_FRONTEND_MEM
- 0x815C STALL_FRONTEND_TLB
- 0x8160 STALL_FRONTEND_CPUBOUND
- 0x8161 STALL_FRONTEND_FLOW
- 0x8162 STALL_FRONTEND_FLUSH
- 0x8164 STALL_BACKEND_MEMBOUND
- 0x8165 STALL_BACKEND_L1D
- 0x8167 STALL_BACKEND_TLB
- 0x8168 STALL_BACKEND_ST
- 0x816B STALL_BACKEND_BUSY
- 0x816C STALL_BACKEND_ILOCK
- 0x818D BUS_REQ_RD
- 0x81BC L1D_CACHE_REFILL_HWPRF
- 0x81BD L2D_CACHE_REFILL_HWPRF
- 0x82FA DTLB_WALK_HWPRF

Configurations Affected

All configurations are affected.

Conditions

- Trace unit is configured to use the extended input facility with an affected event
- The affected event is not enabled for counting in the PMU through the PMEVTYPER<n>EL0 registers

Implications

The affected events cannot be used reliably by the trace unit unless the PMU is also configured to count the same event.

Workaround

This erratum can be avoided if the PMU is configured to count the event selected by the trace unit.

2708967
Read value of PMMIR is incorrect

Status

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

Description

Due to this errata, the BUS_SLOTS and BUS_WIDTH fields of the PMMIR_EL1 system register read as 0 instead of their documented intended values, 0b0010 and 0b0110 respectively. All other fields have their intended value. The incorrect values are also read from the memory-mapped external register, PMMIR.

Configurations Affected

All configurations are affected.

Conditions

The values read for these fields are always incorrect.

Implications

A 0 value in these fields is valid and indicates that the information is not available to software. Software has less information about the BUS_ACCESS performance event than intended.

Workaround

This erratum has no workaround.

2710075
Read value of IMP_CPUCFR_EL1 might be incorrect

Status

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

Description

Due to this errata, several fields of the IMP_CPUCFR_EL1 system register always read as 0 instead of their intended value. The affected fields are:

- L2_RAM_EVA
- L2_NUM_RAMCTL_PARTITIONS
- L2_NUM_TAGCTL_SLICES

Configurations Affected

The values in these fields will match configurations where L2_RAM_EVA is FALSE, and L2_NUM_RAMCTL_PARTITIONS and L2_NUM_TAGCTL_SLICES are both set to 1. All other configurations will have an incorrect value at least one of these fields.

Conditions

For affected configurations, IMP_CPUCFR_EL1 fields with an incorrect value will always be incorrect.

Implications

The information provided by this register might not match the configuration of the L2 cache. Software is not expected to rely on these values.

Workaround

There is no workaround.

2713358
ERRxSTATUS.UET field might be incorrect

Status

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

Description

ERR2STATUS register contain information about reported errors. Under some conditions, the value of the UET field might be incorrect.

Configurations Affected

All configurations are affected.

Conditions

If CORE_CACHE_PROTECTION = 'b1:

- An external abort is detected on a clean, L2 cache allocating line.
- At the same time, a double-bit error is detected on L2 TAGRAMs or L2 L1 Duplicate TAGRAMs.

If CORE_CACHE_PROTECTION = 'b0:

- An external abort is detected on a clean, L2 cache allocating line.

Implications

There is still substantial benefit being gained from the ECC logic. There might be a negligible increase in overall system failure rate due to this erratum.
If the conditions occur with CORE_CACHE_PROTECTION = 'b1, the reported error might record UEO instead of UC on ERR2STATUS.UET.
If the condition occur with CORE_CACHE_PROTECTION = 'b0, the reported error might record UC instead of UEO on ERR2STATUS.UET.

Workaround

There is no workaround required.

2713644
Cache debug target for L2 Data RAM may not record correct data

Status

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

Description

Cache debug target for L2 data RAM might not record the correct data for the top half of a cache line.

Configurations Affected

All configurations with CORE_CACHE_PROTECTION set to False are affected.

Conditions

Software executes a cache debug read targeting the L2 data RAM using SYS #6, C15, C4, #3{, <Xt>}.

Implications

The cache debug data recorded in the IMP_CDBGDR0_EL3 register for the L2 data RAM top half cache line will always be 0, and not reflect the value in the data RAM.

Workaround

There is no workaround required.

2732181
ERR2STATUS might be incorrect

Status

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

Description

The ERR2STATUS register contains information about reported errors. Under some conditions, the value of the register might be incorrect.

Configurations Affected

All configurations are affected.

Conditions

If CORE_CACHE_PROTECTION = FALSE:

- A L2 allocating line is received with poison.

If CORE_CACHE_PROTECTION = TRUE:

- A write to the ERR2STATUS register is performed.

Implications

There is still substantial benefit being gained from the ECC logic. There might be a negligible increase in overall system failure rate due to this erratum.
If the condition with CORE_CACHE_PROTECTION = FALSE is met:

- The PN field is incorrectly set to 0.

If the condition with CORE_CACHE_PROTECTION = TRUE is met:

- The write is performed while the OF field is set and the write is not clearing it.

Workaround

There is no workaround required.

2740664
PMU event 0x77 CRYPTO_SPEC does not always count when enabled

Status

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

Description

The PMU event 0x77 CRYPTO_SPEC does not always count when enabled.

Configurations Affected

This erratum affects all configurations.

Conditions

Under the following condition, PMU event 0x77 CRYPTO_SPEC will never count:

- PMU is configured to count event 0x77, and no events in the range 0x78 to 0xBF are enabled for counting.

Otherwise, the event is counted as expected.

Implications

PMU event 0x77 CRYPTO_SPEC cannot be used without using the software workaround.

Workaround

This erratum can be avoided if the PMU is configured to count an event in the range 0x78 to 0xBF.

2751027
Load operation might abort unexpectedly when accessing poisoned data

Status

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

Description

Load (or atomic load) might abort data accesses when the operation does not access the poisoned data, but the 256 bits aligned data it accesses contain poisoned data.

Configurations Affected

This erratum affects all configurations.

Conditions

1. The core executes a load (or atomic load) operation
2. The load operation miss in L1 cache
3. A part of the returned data contains poisoned data

Implications

If the previous conditions are met, the load (or atomic load) instruction might generate synchronous external Data Abort, even if the chunk of data it accesses does not contain poisoned data.
For atomic load instruction, this means the memory might be updated by the atomic instruction but it still generates precise abort for the atomic instruction.

Workaround

No workaround is required for this erratum.

2803663
Speculative dirty bit hardware update might happen for store operation

Status

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

Description

Speculative dirty bit hardware update might happen during a store operation.

Configurations Affected

This erratum affects configurations where the CORE_CACHE_PROTECTION parameter is TRUE.

Conditions

This erratum occurs under the following conditions:

1. Load operation A
2. Store operation B, following load operation A
3. Hardware update of the dirty bit is enabled for the page of memory accessed by the store operation B
4. Load operation A encounters a potentially correctable ECC error in the L1 data cache, the load operation is microarchitecturally replayed. The erratum occurs If during the replay, the load sees an abort that was not present in the original execution.
5. Timing sensitive microarchitectural condition happens

Implications

If the previous conditions are met, the Store operation might update the AP[2] or S2AP[1] bit as writable when it should not.

There is still substantial benefit being gained from the ECC logic. There might be a negligible increase in overall system failure rate due to this erratum.

Workaround

No workaround is required for this erratum.

2833401
Direct access to internal memory might not be reliable

Status

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

Description

Internal memory used by structures in the L2 cache can be read using system registers. In some conditions, the read value might not reflect the value stored in the memory.

Configurations Affected

This erratum affects configurations having the parameter CORE_CACHE_PROTECTION set to TRUE.

Conditions

1. A core is active.
2. A stream of cache debug operations is issued, using system registers IMP_CDBGL2CMR and IMP_CDBGL2CDR, while the memory system is processing loads and stores to Normal memory.
3. An *Error Correcting Code* (ECC) error is detected in the L2 DATA RAM.
4. Complex microarchitectural timing conditions occur.

Implications

Arm expects that the memory system is in a quiescent state while direct access to memory is being performed.
If the conditions occur, the values read while directly accessing internal memory might not be correct.

Workaround

No workaround is required.

2841875
An uncontainable error might deadlock the cluster

Status

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

Description

An uncontainable error detected when a core is doing a line upgrade might deadlock the cluster.

Configurations Affected

This erratum affects all configurations.

Conditions

1. A core is doing a store that requires a line upgrade.
2. Unlikely, timing-sensitive, microarchitectural conditions occur, including an uncontainable error detected in the L1 Duplicate Tag RAMs.

Implications

There is still substantial benefit being gained from the *Error Correcting Code* (ECC) logic. There might be a negligible increase in overall system failure rate due to this erratum.
If the conditions occur, the complex might deadlock.

Workaround

There is no workaround.

2853709
Error record registers indicate incorrect feature support in configurations without cache protection

Status

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

Description

The following error record feature registers contain information about the features implemented in the corresponding RAS node. The affected nodes are Node 1 (L1 memory system) and Node 2 (L2 memory system).

- **ERR1FR**
- **ERR1PFGF**
- **ERR2FR**
- **ERR2PFGF**

In configurations without cache protection, these registers incorrectly indicate that cache protection is present. This also applies when reading the **ERXFR_EL1** and **ERXPFGF_EL1** registers while **ERRSELR_EL1** is selecting any of the affected nodes. Indication of support for error types caused by External aborts is unaffected.

Also, in the **ERR1PFGCTL** and **ERR2PFGCTL** pseudo-fault generation control registers, fields which control the injection of cache protection error types can be read and written as if support is present. Attempting to inject an unsupported error type will have no effect on pseudo-fault generation.

Configurations Affected

All configurations with the **CORE_CACHE_PROTECTION** parameter set to FALSE are affected.

Conditions

The incorrect read and write behavior of these registers in affected configurations is always present.

Implications

In configurations without cache protection, software might incorrectly assume from these register values that it is actually present. This might lead to an unexpected error injection test result, if a test attempts to inject an error type which it thinks is supported, but no error record is created.

Workaround

This erratum has no workaround. Contact Arm for more details on which error types are not supported when cache protection is not present.

2861633
Some PMU events are incorrectly masked to trace unit

Status

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

Description

Common architectural and microarchitectural *Performance Monitoring Unit* (PMU) events are available to the trace unit through the extended input facility. Due to this erratum, under certain conditions, some events might not be sent to the trace unit after being selected:

- 0x4020 LDST_ALIGN_LAT
- 0x4021 LD_ALIGN_LAT
- 0x4022 ST_ALIGN_LAT
- 0x4024 MEM_ACCESS_CHECKED
- 0x4025 MEM_ACCESS_CHECKED_RD
- 0x4026 MEM_ACCESS_CHECKED_WR

Configurations Affected

All configurations are affected.

Conditions

The erratum occurs when all of the following conditions are met:

- Trace unit is configured to use the extended input facility with an affected event.
- Performance Monitors are disabled because they have been configured to be disabled at EL3 or in Secure state.
- Self-hosted trace is enabled.

Implications

The affected events cannot be used reliably by the trace unit at EL3 or in Secure state unless the Performance Monitors are enabled.

Workaround

There is no workaround.

2871911
LDG or MTE checked load/store might fail to detect poisoned data

Status

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

Description

An LDG or MTE checked load/store might fail to detect poisoned data.

Configurations Affected

This erratum affects configurations with BROADCASTMTE = TRUE.

Conditions

The erratum occurs under the following conditions:

1. An older STG or store operation to cache line X.
2. A younger LDG or MTE checked load/store to the same cache line X.
3. Cache line X has a deferred error.
4. Timing sensitive, microarchitectural conditions occur.

Implications

If the conditions are met, the LDG or MTE checked load/store might fail to detect poisoned data, and might return an incorrect result for an LDG, or an incorrect tag check result for a checked load or store. If asynchronous MTE tag checks are enabled, the state of TFSR_ELx might get corrupted.

Workaround

No workaround is required for this erratum.

2872870
CE or DE errors from L1 data cache access might not be recorded in the RAS records

Status

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

Description

A corrected or deferred error detected during an access to the data or MTE RAMs of the L1 data cache might not be reported to RAS.

Configurations Affected

This erratum affects all configurations with parameter CORE_CACHE_PROTECTION set to TRUE.

Conditions

1. A line is cached in L1 in shared clean state.
2. An error is detected in the data or MTE RAMs of the L1 data cache while accessing the line.

Implications

There is still substantial benefit being gained from the *Error Correcting Code* (ECC) logic. There might be a negligible increase in overall system failure rate due to this erratum.
If the conditions occur, CE and DE detected when accessing the data or MTE RAMs of the L1 data cache will not be recorded in the RAS node. Error correction functionality and aborts handling are not affected by this erratum.

Workaround

There is no workaround.

2879977
Unmodified cache line might be written back to memory

Status

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

Description

A cache line might be temporarily marked as modified, which might result in that line being written back to memory.

Configurations affected

This erratum affects all configurations with parameter BROADCASTMTE set to True.

Conditions

This erratum occurs under the following conditions:

1. Memory location A is marked as Normal Inner Write-Back, Outer Write-Back Cacheable memory.
2. The core allocates location A into the L1 data cache or the L2 cache in Unique state without MTE tags. This allocation might be due to committed instructions, speculative execution, or data prefetching.
3. The core executes an STG, ST2G, or STGM that requires fetching of MTE tags by the L2.
4. Another *Request Node* (RN) is requesting the line, and this request is ordered before the previous condition (3) in the *Home Node* (HN). The core will provide the line as dirty, but data remains unchanged.

Implications

If the previous conditions are met, the cache line for memory location A might be marked as modified, but the data remains unchanged.
If the line is evicted to memory while set as dirty with unchanged data, it will then overwrite the value in memory. If an agent in the system has written to location A through a Non-cacheable mapping, these writes might then be overwritten with the older data from the core cache write-back, causing these writes to no longer be visible. This might then result in data corruption for software-managed coherency use cases.
The scenario is a race conditions where an old value of location A can be temporarily seen by a Non-cacheable observer. If the core executes a read to memory location A before the store, that is requiring a DC IVAC (Data or unified Cache line Invalidate by VA to PoC), the race condition is resolved, and the erratum is not applicable.

Workaround

No workaround is required for this erratum.

2940628
Store data might be lost when a correctable error is detected in the L1 data cache

Status

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

Description

Store data might be lost when a correctable error is detected in the L1 data cache RAM or L1 data cache *Memory Tagging Extension* (MTE) tag RAM.

Configurations affected

This erratum affects configurations with CPU_CACHE_PROTECTION set.

Conditions

This erratum occurs under the following conditions:

1. The core executes two or more stores to the same cache line but to different 16B-aligned quantities. At least one of the stores is a store of less than 32 bits, or is MTE tag-checked.
2. The partial or MTE tag-checked store above sees a correctable *Error Correcting Code* (ECC) error in the L1 data cache RAM or L1 data cache MTE tag RAM.
3. Very unlikely, timing-sensitive micro-architectural conditions occur.

Implications

There is still substantial benefit being gained from the ECC logic. There might be a negligible increase in overall system failure rate due to this erratum.

If the conditions are met, a single-bit error could result in silent data corruption. This is similar to the case of a triple-bit error incorrectly being detected as a single-bit error.

One of the stores at condition (1) can write to the cache without marking the cache line as dirty. A second store that must already be in the store buffer will shortly mark the line dirty, but the line can be lost from the *Processing Element* (PE) caches in the small window between both operations. If the cache line leaves the PE caches in this window, the data from the store that has already been written to the cache might be lost, as it is not marked as dirty.

Workaround

No workaround is required.

2969138
Unmodified page table cache lines might be written back to memory

Status

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

Description

Hardware management of the Access Flag or Dirty State might set a cache line containing page table data as dirty even if the descriptor data has not been modified.

Configurations affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. Hardware management of the Access Flag is enabled (TCR_ELx.HA or VTCR_EL2.HA are set to 0b1) or Hardware management of the Dirty State is enabled (TCR_ELx.HD or VTCR_EL2.HD are set to 0b1).
2. The *Processing Element* (PE) schedules an Access Flag or Dirty State update after having read a descriptor.
3. The descriptor changes before the hardware update is performed, and one of the following conditions applies to the new descriptor:
    - It is not a page or block descriptor anymore.
    - It does not have the DBM bit set.
    - It has different permissions than the old descriptor.

Implications

If the conditions are met, the descriptor will not be modified, but the line will be marked as dirty. If the stage 1 hardware update of the access flag or dirty bit fails because of a stage 2 fault, the issue does not occur.

The cache line will be written back to main memory when evicted from the PE, which can result in a negligible increase in system power.

Workaround

No workaround is required.

