



Arm Cortex-X2 (MP121)

Software Developer Errata Notice

Date of issue: December 15, 2023

Non-Confidential

Document version: 18.0

Copyright © 2023 Arm® Limited (or its affiliates). All rights reserved.

Document ID: SDEN-1775100

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



Non-confidential proprietary notice

This document is protected by copyright and other related rights and the practice or implementation of the information contained in this document may be protected by one or more patents or pending patent applications. No part of this document may be reproduced in any form by any means without the express prior written permission of Arm. No license, express or implied, by estoppel or otherwise to any intellectual property rights is granted by this document unless specifically stated.

Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether implementations infringe any third party patents.

THIS DOCUMENT IS PROVIDED "AS IS". ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, third party patents, copyrights, trade secrets, or other rights.

This document may include technical inaccuracies or typographical errors.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document consists solely of commercial items. You shall be responsible for ensuring that any use, duplication or disclosure of this document complies fully with any relevant export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word "partner" in reference to Arm's customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

If any of the provisions contained in these terms conflict with any of the provisions of any click through or signed written agreement covering this document with Arm, then the click through or signed written agreement prevails over and supersedes the conflicting provisions of these terms. This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of the Agreement shall prevail.

The Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners. Please follow Arm's trademark usage guidelines at <https://www.arm.com/company/policies/trademarks>.

Copyright © 2023 Arm® Limited (or its affiliates). All rights reserved.

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-X2 (MP121), 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

r2p0 implementation fixes	11
Introduction	12
Scope	12
Categorization of errata	12
Change Control	13
Errata summary table	26
Errata descriptions	37
Category A	37
1791789 Fault info captured in FAR and ESR registers for LDP 64-bit variant might be incorrect	37
Category A (rare)	38
Category B	39
1785648 Atomic store instructions to shareable write-back memory might cause memory consistency failures	39
1793423 An unexpected data abort might occur under specific micro-architectural conditions following an abort on an earlier instruction	40
1801992 Hardware Access/Dirty flag updates might indicate successful completion, but PTE is not updated	41
1813969 TLBI range instructions with NUM>31 may not invalidate all required entries+	42
1863568 Core might generate Breakpoint exception on incorrect IA	43
1887102 IPA based TLB Invalidate might fail to invalidate translation table entries caching translations for the Trace Buffer Extension	44
1887413 Executing a SVE load with no active predicates might result in a deadlock under certain micro-architectural conditions	45
1890822 Stage 2 abort during Secure EL1 translation might report incorrect NS value in HPFAR_EL2	46
1901946 Executing software prefetch instructions from a context with memory tagging enabled might lead to corruption of architecture state	47
1906301 Core might deadlock when memory-mapped read to Debug/Trace/PMU register is followed by WFI or WFE	48
1914047 External debugger access to Debug registers might not work during Warm reset	49
1916945 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	50
1917258 Non-fault SVE load does not update FFR when it reads data with ECC error or external abort	51
1918765 CFP RCTX and CPP RCTX instructions might incorrectly execute as a NOP in ELO	52

1927200	Atomic instructions with acquire semantics might not be ordered with respect to older stores with release semantics	53
1934260	Tag checked streaming write might report false fail	55
1984319	Incorrect read value for Performance Monitors Common Event Identification register	56
2002765	Embedded Trace of WFI or WFE instructions might corrupt PE architectural state	58
2008768	RAS errors during core power down might cause a deadlock	60
2012097	TRBE writes to MTE tagged pages might not report external aborts	62
2017096	Streaming STG and STG2 performance lower than expected with TCF=NONE	63
2023111	Utility Bus register accesses to reserved addresses of PE might hang	64
2054223	The trace data is not flushed completely during a TSB instruction executed in prohibited region	65
2058056	Disabling of data prefetcher with outstanding prefetch TLB miss might cause a deadlock	66
2081180	Executing a WFI or WFE instruction after a STREX instruction might result in a deadlock under specific conditions	67
2083908	Execution of ST2G instructions in close proximity might cause loss of MTE allocation tag data	69
2119858	Trace data might get overwritten in TRBE FILL mode	70
2136059	The CPP instruction will apply to an incorrect EL context	71
2147715	A CFP instruction might not invalidate the correct resources	72
2216384	PDP deadlock due to CMP/CMN + B.AL/B.NV fusion	73
2219376	Enabling TRBE might cause a data write to a page with the wrong ASID when owning Exception level is EL1	74
2224489	TRBE might cause a data write to an out-of-range address which is not reserved for TRBE	76
2267065	A CFP instruction might execute with incorrect upper ASID or VMID bits	77
2282622	Continuous failing STREX because of another PE executing prefetch for store behind consistently mispredicted branch	78
2291219	Denied power down request might prevent completion of future power down request	79
2371105	Translation table walk folding into an L1 prefetch might cause data corruption	80
2381390	A continuous stream of incoming DVM syncs may cause TRBE to prevent the core from forward progressing	81
2701952	The core might fetch stale instruction from memory when both Stage 1 Translation and Instruction Cache are Disabled with Stage 2 forced Write-Back	82
2742423	Page crossing access that generates an MMU fault on the second page could result in a livelock	84
2768515	The core might deadlock during powerdown sequence	85

2778471	The PE might generate memory accesses using invalidated mappings after completion of a DVM SYNC operation.	86
3003018	PE executing DRPS during Debug Halt under Double Fault condition will not execute properly	87
3038569	TRBE might write to pages which lack write permission at Stage-1 or Stage-2	88
3099212	PE might execute instructions consistent with previous context-synchronized state when SCR_EL3.EEL2 is changed	90
Category B (rare)		92
2982956	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	92
Category C		94
1786338	Memory uploads and downloads via memory access mode within Debug state can fail to accurately read or write memory contents	94
1787272	TSB instruction completion can be delayed when executed in region where trace is allowed	96
1799975	Watchpoint Exception on DC ZVA does not report correct address in FAR or EDWAR	97
1804175	CTI event from the core to the external DebugBlock might be dropped	98
1804563	Trace Buffer Extension unit might write trace packets to memory using incorrect memory page attributes	99
1817593	Persistent faults on speculative elements of SVE First-fault gather-load instructions might result in deadlock	100
1827136	External debug accesses in memory access mode with SCTLRL_ELx.IESB set might result in unpredictable behavior	101
1838906	Noncompliance with prioritization of Exception Catch debug events	102
1851171	Transient L2 tag double bit Errors might cause data corruption	104
1851323	Incorrect trace timestamp value when self-hosted trace is disabled	105
1851816	The MPAM value associated with MMU descriptor fetch requests might be incorrect	106
1855551	ERRORMISC0_EL1.SUBARRAY, ERRORSTATUS.CE, and ERRORSTATUS.DE values for ECC errors in the L1 data cache might be incorrect	106
1859562	Incorrect read value for the Trace ID Register 3 SYSSTALL field	108
1862651	Incorrect read value for External Debug Processor Feature Register	109
1865453	The values for fields ID_AA64ZFR0_EL1.{SM4,SHA3,AES} read incorrectly as non-zero	110
1868638	The core does not treat the BAS field of the Debug Breakpoint Control Register as RES1	111
1870363	L2 data RAM may fail to report corrected ECC errors	112

1875555	Compare and Swap (CAS) instructions with stack pointer as base register are incorrectly treated as checked accesses	113
1875745	A Checked load that fails a Tag Check could set the ESR to an incorrect value	114
1884880	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	115
1893664	Accessing a memory location using mismatched shareability attributes when MTE tag checking is enabled might lose coherency or deadlock	116
1896171	Access to External Debug Auxiliary Processor Feature Register might incorrectly return an error response	117
1899211	Some corrected errors might incorrectly increment ERR0MISC0.CECR or ERR0MISC0.CECO	118
1899435	PFG duplicate reported faults through a Warm reset	119
1909702	IDATAn_EL3 might represent incorrect value after direct memory access to internal memory for Instruction TLB	120
1911676	TFSR contents might be incorrect after executing a page crossing SVE predicated load instruction	121
1919240	The PE might deadlock if Pseudofault Injection is enabled in Debug State	122
1920415	Trace Buffer might write trace packets to memory using incorrect cache attributes	123
1920634	A Checked store with poisoned tags might result in a Tag Check Fail instead of taking an SError interrupt exception	124
1920871	MPAM value associated with translation table walk request might be incorrect	125
1925506	Unsupported atomic fault due to memory type defined in first stage of translation might result in exception being taken to EL2	126
1926908	Access with additional latency from alignment (LDST_ALIGN_LAT) PMU event does not count	127
1927566	ERR0MISC0_EL1.SUBARRAY value for ECC errors in the L1 data cache might be incorrect	128
1929989	Event Stream from the Virtual Counter is not correctly disabled by VHE in Secure State	129
1938354	Incorrect fault status code might be reported in Trace Buffer Extension register TRBSR_EL1.FSC	130
1949697	A Checked store that crosses a page boundary might not perform a Tag Check	131
1971496	VMID value in trace packets might be incorrect	132
1975917	AMU Event 0x0011, Core frequency cycles might increment incorrectly when the core is in WFI or WFE state	133
1980906	Reset Catch debug event might not cause core to enter Debug state immediately after Cold reset	135
1986267	DRPS might not execute correctly in Debug state with SCTLRL_ELx.IESB set in the current EL	136

1989365	Floating-point Operations speculatively executed PMU events are not counted	137
2000010	Execution of STG instructions in close proximity might incorrectly write MTE Allocation Tag to memory more than once	138
2002779	CPU might fetch incorrect instruction from a page programmed as non-cacheable in stage-1 translation and as device memory in stage-2 translation	139
2017087	DSB might not guarantee completion of direct reads of L2 cache memories	140
2018317	External APB write to a register located at offset 0x084 might incorrectly issue a write to External Debug Instruction Transfer Register	141
2025108	Corrupted register state results from executing specific form of SEL instruction followed by SVE AESMC or AESIMC instruction	143
2050953	External aborts for streaming writes to MTE tagged pages may report multiple errors	144
2052424	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	145
2054222	Trace data lost during collection stop in TRBE	147
2058367	L3D_CACHE_ALLOC PMU inaccurate when using WriteEvictOrEvict transactions	148
2058540	Incorrect Fault Status code reported for predicated SVE op	149
2061107	Tag check fail might not be reported for an unaligned predicated SVE store	150
2089668	OSECRR_EL1/EDECRR is incorrectly included in the Warm Reset domain	151
2093019	Extra A-sync packet might get written to Trace Buffer in Trace prohibited region	152
2109742	Speculative access to a recently unmapped physical address previously containing page tables might occur	153
2112535	L1D_CACHE_INVALID and L2D_CACHE_INVALID PMU events fail to increment for SnpPreferUnique and SnpPreferUniqueFwd	154
2113481	MPAM value associated with instruction fetch might be incorrect	155
2117983	Data abort on SVE first fault load might be routed to incorrect Exception level	156
2141645	A64 WFI or A64 WFE executed in Debug state suspends execution indefinitely	157
2143136	Some SVE PMU events count incorrectly	159
2146514	PMU Event MEM_ACCESS_CHECKED_WR, 0x4026 counts incorrectly and MEM_ACC_CHECKED 0x4024 might be incorrect	161
2154216	FAR_ELx contents for a Data Abort exception on SVE first fault contiguous load instruction due to Tag Check fail might be incorrect	162
2159150	Direct access of L2 data RAMs using RAMINDEX returns incomplete data	163
2174188	PMU_HOVFS event not always exported when self-hosted trace is disabled	164
2178034	An SError might not be reported for an atomic store that encounters data poison	165
2186347	64 bit source SVE PMULLB/T not considered Cryptography instruction	166
2227174	Streaming writes to memory mapped Non-shareable and write-back might cause data corruption because of reordering	167

2238108	Read or write from Secure EL1 for ICV_BPR1_EL1 register might not work	168
2238111	Reads of DISR_EL1 incorrectly return 0s while in Debug State	169
2239139	DRPS instruction is not treated as UNDEFINED at EL0 in Debug state	170
2243871	ELR_ELx[63:48] might hold incorrect value when PE disables address translation	171
2245716	TRBE might use incorrect Cacheability attributes for TRBE data when address translation is disabled	172
2245832	ESR_ELx contents for a Data Abort exception might be incorrect when an L1D tag double bit error is encountered	173
2247178	L1 MTE Tag poison is not cleared	174
2254450	L1 Data poison is not cleared by a store	175
2276444	PMU event for full/partial/empty/not full predicate incorrect for some SVE instructions	176
2278134	PMU L1D_CACHE_REFILL_OUTER is inaccurate	177
2283666	Lower priority exception might be reported when abort condition is detected at both stages of translation	178
2307829	ESR_ELx.ISV can be set incorrectly for an external abort on translation table walk	179
2317617	ESR_ELx contents for a Data Abort exception might be incorrect when a data double bit error or external abort is encountered	180
2334390	L2 tag RAM double-bit ECC error might lead to the PE not responding to a forwarding snoop	181
2344960	CSSELR_EL1.TnD is RAZ/WI when CSSELR_EL1.InD == 0x1	182
2382765	Incorrect read value for Performance Monitors Configuration Register	183
2391680	Software-step not done after exit from Debug state with an illegal value in DSPSR	184
2444421	PMU STALL_SLOT_BACKEND and STALL_SLOT_FRONTEND events count incorrectly	185
2643627	ERXPFgcdn_EL1 register is incorrectly written on Warm reset	186
2647274	Incorrect read value for Performance Monitors Control Register	187
2652240	FAR_ELx contents for a Data Abort exception on SVE first fault contiguous load instruction due to Tag Check fail might be incorrect	188
2676362	Execution of STG instructions in close proximity might cause loss of MTE allocation tag data	189
2692441	L3D PMU events may be inaccurate	190
2694769	MTE checked load might read an old value of allocation tag by not complying with address dependency ordering	191
2712632	Incorrect read value for Performance Monitors Configuration Register EX field	192
2726256	IRG instructions might produce the wrong tag when GCR_EL1.RRND=0x0.	193
2769023	STALL_BACKEND_MEM, Memory stall cycles AMU event count incorrectly	194
2798805	Incorrect decoding of SVE version of PRF* scalar plus scalar instructions	195

2799687	ECC errors in MTE allocation tags may lead to silent data corruption in tag values	197
2814414	Incorrect timestamp value reported in SPE records when timestamp capture is enabled	198
2814418	PE might fail to detect multiple uncorrectable ECC errors in the L1 data cache tag RAM	199
2817889	TRBE buffer write translation out of context may have incorrect memory attributes	200
2910963	L2D_CACHE_WB_CLEAN overcounts	201
2921487	Accessing a memory location using mismatched Shareability attributes when MTE tag checking is enabled might cause data corruption	202
3061569	TagMatch responses with error indication do not generate a SError abort	203

r2p0 implementation fixes

Note the following errata might be fixed in some implementations of r2p0. This can be determined by reading the REVIDR_EL1 register where a set bit indicates that the erratum is fixed in this part.

REVIDR_EL1[0]	1791789 Fault info captured in FAR and ESR registers for LDP 64-bit variant could be incorrect
REVIDR_EL1[1]	1975917 AMU Event 0x0011, Core frequency cycles might increment incorrectly when core is in WFI or WFE state
REVIDR_EL1[2]	1980906 Reset Catch debug event might not cause core to enter Debug state immediately after Cold reset
REVIDR_EL1[3]	2017096 Streaming STG and STG2 performance lower than expected with TCF=NONE

Note that there is no change to the MIDR_EL1 which remains at r2p0. Software will identify this release through the combination of MIDR_EL1 and REVIDR_EL1.

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.

December 15, 2023: Changes in document version v18.0

ID	Status	Area	Category	Summary
3038569	Updated	Programmer	Category B	TRBE might write to pages which lack write permission at Stage-1 or Stage-2
3099212	New	Programmer	Category B	PE might execute instructions consistent with previous context-synchronized state when SCR_EL3.EEL2 is changed
3061569	New	Programmer	Category C	TagMatch responses with error indication do not generate a SError abort

September 01, 2023: Changes in document version v17.0

ID	Status	Area	Category	Summary
3003018	New	Programmer	Category B	PE executing DRPS during Debug Halt under Double Fault condition will not execute properly
3038569	New	Programmer	Category B	TRBE might write to pages which lack write permission at Stage-1 or Stage-2
2982956	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
2726256	New	Programmer	Category C	IRG instructions might produce the wrong tag when GCR_EL1.RRND=0x0
2910963	New	Programmer	Category C	L2D_CACHE_WB_CLEAN overcounts
2921487	New	Programmer	Category C	Accessing a memory location using mismatched Shareability attributes when MTE tag checking is enabled might cause data corruption

February 22, 2023: Changes in document version v16.0

ID	Status	Area	Category	Summary
2798805	New	Programmer	Category C	Incorrect decoding of SVE version of PRF* scalar plus scalar instructions
2799687	New	Programmer	Category C	ECC errors in MTE allocation tags may lead to silent data corruption in tag values
2814414	New	Programmer	Category C	Incorrect timestamp value reported in SPE records when timestamp capture is enabled
2814418	New	Programmer	Category C	PE may fail to detect multiple uncorrectable ECC errors in the L1 data cache tag RAM
2817889	New	Programmer	Category C	TRBE buffer write translation out of context may have incorrect memory attributes

November 01, 2022: Changes in document version v15.0

ID	Status	Area	Category	Summary
2742423	New	Programmer	Category B	Page crossing access that generates an MMU fault on the second page could result in a livelock
2768515	New	Programmer	Category B	The core might deadlock during powerdown sequence
2778471	New	Programmer	Category B	The PE might generate memory accesses using invalidated mappings after completion of a DVM SYNC operation
1975917	Updated	Programmer	Category C	AMU Event 0x0011, Core frequency cycles might increment incorrectly when the core is in WFI or WFE state
2769023	New	Programmer	Category C	STALL_BACKEND_MEM, Memory stall cycles AMU event count incorrectly

September 09, 2022: Changes in document version v14.0

ID	Status	Area	Category	Summary
2282622	Updated	Programmer	Category B	Continuous failing STREX because of another PE executing prefetch for store behind consistently mispredicted branch
2701952	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
2652240	New	Programmer	Category C	FAR_ELx contents for a Data Abort exception on SVE first fault contiguous load instruction due to Tag Check fail might be incorrect
2676362	New	Programmer	Category C	Execution of STG instructions in close proximity might cause loss of MTE allocation tag data
2692441	New	Programmer	Category C	L3D PMU events may be inaccurate
2694769	New	Programmer	Category C	MTE checked load might read an old value of allocation tag by not complying with address dependency ordering
2712632	New	Programmer	Category C	Incorrect read value for Performance Monitors Configuration Register EX field

May 26, 2022: Changes in document version v13.0

ID	Status	Area	Category	Summary
2391680	New	Programmer	Category C	Software-step not done after exit from Debug state with an illegal value in DSPSR
2444421	New	Programmer	Category C	PMU STALL_SLOT_BACKEND and STALL_SLOT_FRONTEND events count incorrectly
2643627	New	Programmer	Category C	ERXPFPGCDN_EL1 register is incorrectly written on Warm reset
2647274	New	Programmer	Category C	Incorrect read value for Performance Monitors Control Register

December 16, 2021: Changes in document version v12.0

ID	Status	Area	Category	Summary
1791789	Updated	Programmer	Category A	Fault info captured in FAR and ESR registers for LDP 64-bit variant could be incorrect
1984319	Updated	Programmer	Category B	Incorrect read value for Performance Monitors Common Event Identification Register

ID	Status	Area	Category	Summary
2002765	Updated	Programmer	Category B	Embedded Trace of WFI or WFE instructions might corrupt PE architectural state
2008768	Updated	Programmer	Category B	RAS errors during core power down might cause a deadlock
2012097	Updated	Programmer	Category B	TRBE writes to MTE tagged pages might not report external aborts
2017096	Updated	Programmer	Category B	Streaming STG and STG2 performance lower than expected with TCF=NONE
2023111	Updated	Programmer	Category B	Utility Bus register accesses to reserved addresses of PE might hang
2054223	Updated	Programmer	Category B	The trace data is not flushed completely during a TSB instruction executed in prohibited region
2081180	Updated	Programmer	Category B	Executing a WFI or WFE instruction after a STREX instruction might result in a deadlock under specific conditions
2083908	Updated	Programmer	Category B	Execution of ST2G instructions in close proximity might cause loss of MTE allocation tag data
2119858	Updated	Programmer	Category B	Trace data might get overwritten in TRBE FILL mode
2136059	Updated	Programmer	Category B	The CPP instruction will apply to an incorrect EL context
2147715	Updated	Programmer	Category B	A CFP instruction might not invalidate the correct resources
2216384	Updated	Programmer	Category B	PDP deadlock due to CMP/CMN + B.AL/B.NV fusion
2219376	Updated	Programmer	Category B	Enabling TRBE might cause a data write to a page with the wrong ASID when owning Exception level is EL1
2224489	Updated	Programmer	Category B	TRBE might cause a data write to an out-of-range address which is not reserved for TRBE
2267065	Updated	Programmer	Category B	A CFP instruction might execute with incorrect upper ASID or VMID bits
2282622	New	Programmer	Category B	Continuous failing STREX because of another PE executing prefetch for store behind consistently mispredicted branch
2291219	Updated	Programmer	Category B	Denied power down request might prevent completion of future power down request
2371105	New	Programmer	Category B	Translation table walk folding into an L1 prefetch might cause data corruption
2381390	New	Programmer	Category B	A continuous stream of incoming DVM syncs may cause TRBE to prevent the CPU from forward progressing
1899211	Updated	Programmer	Category C	Some corrected errors might incorrectly increment ERR0MISCO.CECCR or ERR0MISCO.CECO
1920871	Updated	Programmer	Category C	MPAM value associated with translation table walk request might be incorrect
1938354	Updated	Programmer	Category C	Incorrect fault status code might be reported in Trace Buffer Extension register TRBSR_EL1.FSC
1911676	Updated	Programmer	Category C	TFSR contents might be incorrect after executing a page crossing SVE predicated load instruction

ID	Status	Area	Category	Summary
1949697	Updated	Programmer	Category C	A Checked store that crosses a page boundary might not perform a Tag Check
1971496	Updated	Programmer	Category C	VMID value in trace packets might be incorrect
1975917	Updated	Programmer	Category C	AMU Event 0x0011, Core frequency cycles might increment incorrectly when the core is in WFI or WFE state
1980906	Updated	Programmer	Category C	Reset Catch debug event might not cause core to enter Debug state immediately after Cold reset
1986267	Updated	Programmer	Category C	DRPS might not execute correctly in Debug state with SCTLR_ELx.IESB set in the current EL
1989365	Updated	Programmer	Category C	Floating-point Operations speculatively executed PMU events are not counted
2000010	Updated	Programmer	Category C	Execution of STG instructions in close proximity might incorrectly write MTE Allocation Tag to memory more than once
2002779	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
2017087	Updated	Programmer	Category C	DSB might not guarantee completion of direct reads of L2 cache memories
2018317	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
2025108	Updated	Programmer	Category C	Corrupted register state results from executing specific form of SEL instruction followed by SVE AESMC or AESIMC instruction
2050953	Updated	Programmer	Category C	External aborts for streaming writes to MTE tagged pages may report multiple errors
2052424	Updated	Programmer	Category C	An execution of MSR instruction might not update the destination register correctly when an external debugger initiates APB write operation to update debug registers
2054222	Updated	Programmer	Category C	Trace data lost during collection stop in TRBE
2058367	Updated	Programmer	Category C	L3D_CACHE_ALLOC PMU inaccurate when using WriteEvictOrEvict transactions
2058540	Updated	Programmer	Category C	Incorrect Fault Status code reported for predicated SVE op
2061107	Updated	Programmer	Category C	Tag check fail might not be reported for an unaligned predicated SVE store
2089668	Updated	Programmer	Category C	OSECRR_EL1/EDECRR is incorrectly included in the Warm Reset domain
2093019	Updated	Programmer	Category C	Extra A-sync packet might get written to Trace Buffer in Trace prohibited region
2109742	Updated	Programmer	Category C	Speculative access to a recently unmapped physical address previously containing page tables might occur
2112535	Updated	Programmer	Category C	L1D_CACHE_INVALID and L2D_CACHE_INVALID PMU events fail to increment for SnpPreferUnique and SnpPreferUniqueFwd
2117983	Updated	Programmer	Category C	Data abort on SVE first fault load might be routed to incorrect Exception level

ID	Status	Area	Category	Summary
2141645	Updated	Programmer	Category C	A64 WFI or A64 WFE executed in Debug state suspends execution indefinitely
2143136	Updated	Programmer	Category C	Some SVE PMU events count incorrectly
2146514	Updated	Programmer	Category C	PMU Event MEM_ACCESS_CHECKED_WR, 0x4026 counts incorrectly and MEM_ACC_CHECKED 0x4024 might be incorrect
2154216	Updated	Programmer	Category C	FAR_ELx contents for a Data Abort exception on SVE first fault contiguous load instruction due to Tag Check fail might be incorrect
2159150	Updated	Programmer	Category C	Direct access of L2 data RAMs using RAMINDEX returns incomplete data
2174188	Updated	Programmer	Category C	PMU_HOVFS event not always exported when self-hosted trace is disabled
2178034	Updated	Programmer	Category C	An SError might not be reported for an atomic store that encounters data poison
2186347	Updated	Programmer	Category C	64 bit source SVE PMULLB/T not considered Cryptography instruction
2227174	Updated	Programmer	Category C	Streaming writes to memory mapped Non-shareable and write-back might cause data corruption because of reordering
2238108	Updated	Programmer	Category C	Read or write from Secure EL1 for ICV_BPR1_EL1 register might not work
2238111	Updated	Programmer	Category C	Reads of DISR_EL1 incorrectly return 0s while in Debug State
2239139	Updated	Programmer	Category C	DRPS instruction is not treated as UNDEFINED at EL0 in Debug state
2243871	Updated	Programmer	Category C	ELR_ELx[63:48] might hold incorrect value when PE disables address translation
2245832	Updated	Programmer	Category C	ESR_ELx contents for a Data Abort exception might be incorrect when an L1D tag double bit error is encountered
2245716	Updated	Programmer	Category C	TRBE might use incorrect Cacheability attributes for TRBE data when address translation is disabled
2247178	Updated	Programmer	Category C	L1 MTE Tag poison is not cleared
2254450	New	Programmer	Category C	L1 Data poison is not cleared by a store
2276444	New	Programmer	Category C	PMU event for full/partial/empty predicate incorrect for some SVE instructions
2278134	New	Programmer	Category C	PMU L1D_CACHE_REFILL_OUTER is inaccurate
2283666	New	Programmer	Category C	Lower priority exception might be reported when abort condition is detected at both stages of translation
2307829	New	Programmer	Category C	ESR_ELx.ISV can be set incorrectly for an external abort on translation table walk
2317617	New	Programmer	Category C	ESR_ELx contents for a Data Abort exception might be incorrect when a data double bit error or external abort is encountered
2334390	New	Programmer	Category C	L2 tag RAM double-bit ECC error might lead to the PE not responding to a forwarding snoop
2344960	New	Programmer	Category C	CSSELR_EL1.TnD is RAZ/WI when CSSELR_EL1.InD == 0x1
2382765	New	Programmer	Category C	Incorrect read value for Performance Monitors Configuration Register

October 08, 2021: Changes in document version v11.0

ID	Status	Area	Category	Summary
2008768	Updated	Programmer	Category B	RAS errors during core power down might cause a deadlock
2147715	Updated	Programmer	Category B	A CFP instruction might not invalidate the correct resources
2267065	New	Programmer	Category B	A CFP instruction might execute with incorrect upper ASID or VMID bits
2291219	New	Programmer	Category B	Denied power down request might prevent completion of future power down request
2141645	Updated	Programmer	Category C	A64 WFI or A64 WFE executed in Debug state suspends execution indefinitely
2227174	Updated	Programmer	Category C	Streaming writes to memory mapped Non-shareable and write-back might cause data corruption because of reordering
2238108	New	Programmer	Category C	Read or write from Secure EL1 for ICV_BPR1_EL1 register might not work
2238111	New	Programmer	Category C	Reads of DISR_EL1 incorrectly return 0s while in Debug State
2239139	New	Programmer	Category C	DRPS instruction is not treated as UNDEFINED at EL0 in Debug state
2243871	New	Programmer	Category C	ELR_ELx[63:48] might hold incorrect value when PE disables address translation
2245716	New	Programmer	Category C	TRBE might use incorrect Cacheability attributes for TRBE data when address translation is disabled
2247178	New	Programmer	Category C	L1 MTE Tag poison is not cleared

July 16, 2021: Changes in document version v10.0

ID	Status	Area	Category	Summary
2147715	New	Programmer	Category B	A CFP instruction might not invalidate the correct resources
2216384	New	Programmer	Category B	PDP deadlock due to CMP/CMN + B.AL/B.NV fusion
2219376	New	Programmer	Category B	Enabling TRBE might cause a data write to a page with the wrong ASID when owning Exception level is EL1
2224489	New	Programmer	Category B	TRBE might cause a data write to an out-of-range address which is not reserved for TRBE
2178034	New	Programmer	Category C	An SError might not be reported for an atomic store that encounters data poison
2186347	New	Programmer	Category C	64 bit source SVE PMULLB/T not considered Cryptography instruction
2227174	New	Programmer	Category C	Streaming writes to memory mapped Non-shareable and write-back might cause data corruption because of reordering
2245832	New	Programmer	Category C	ESR_ELx contents for a Data Abort exception might be incorrect when an L1D tag double bit error is encountered

June 08, 2021: Changes in document version v9.0

ID	Status	Area	Category	Summary
1934260	Updated	Programmer	Category B	Tag checked streaming write might report false fail
2002765	Updated	Programmer	Category B	Embedded Trace of WFI or WFE instructions might corrupt PE architectural state
2136059	New	Programmer	Category B	The CPP instruction will apply to an incorrect EL context
2141645	New	Programmer	Category C	A64 WFI or A64 WFE executed in Debug state suspends execution indefinitely
2143136	New	Programmer	Category C	Some SVE PMU events count incorrectly
2146514	New	Programmer	Category C	PMU Event MEM_ACCESS_CHECKED_WR, 0x4026 counts incorrectly and MEM_ACC_CHECKED 0x4024 might be incorrect
2154216	New	Programmer	Category C	FAR_ELx contents for a Data Abort exception on SVE first fault contiguous load instruction due to Tag Check fail might be incorrect
2159150	New	Programmer	Category C	Direct access of L2 data RAMs using RAMINDEX returns incomplete data
2174188	New	Programmer	Category C	PMU_HOVFS event not always exported when self-hosted trace is disabled

April 14, 2021: Changes in document version v8.0

ID	Status	Area	Category	Summary
1927200	Updated	Programmer	Category B	Atomic instructions with acquire semantics might not be ordered with respect to older stores with release semantics
2058056	New	Programmer	Category B	Disabling of data prefetcher with outstanding prefetch TLB miss might cause a deadlock
2081180	New	Programmer	Category B	Executing a WFI or WFE instruction after a STREX instruction might result in a deadlock under specific conditions
2083908	New	Programmer	Category B	Execution of ST2G instructions in close proximity might cause loss of MTE allocation tag data
2119858	New	Programmer	Category B	Trace data might get overwritten in TRBE FILL mode
2018317	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
2058540	New	Programmer	Category C	Incorrect Fault Status code reported for predicated SVE op
2061107	New	Programmer	Category C	Tag check fail might not be reported for an unaligned predicated SVE store
2089668	New	Programmer	Category C	OSECCR_EL1/EDECCR is incorrectly included in the Warm Reset domain
2093019	New	Programmer	Category C	Extra A-sync packet might get written to Trace Buffer in Trace prohibited region
2109742	New	Programmer	Category C	Speculative access to a recently unmapped physical address previously containing page tables might occur
2112535	New	Programmer	Category C	L1D_CACHE_INVALID and L2D_CACHE_INVALID PMU events fail to increment for SnpPreferUnique and SnpPreferUniqueFwd
2113481	New	Programmer	Category C	MPAM value associated with instruction fetch might be incorrect
2117983	New	Programmer	Category C	Data abort on SVE first fault load might be routed to incorrect Exception level

February 02, 2021: Changes in document version v7.0

ID	Status	Area	Category	Summary
2023111	New	Programmer	Category B	Utility Bus register accesses to reserved addresses of PE might hang
2054223	New	Programmer	Category B	The trace data is not flushed completely during a TSB instruction executed in prohibited region
2002779	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
2050953	New	Programmer	Category C	External aborts for streaming writes to MTE tagged pages may report multiple errors
2052424	New	Programmer	Category C	An execution of MSR instruction might not update the destination register correctly when an external debugger initiates APB write operation to update debug registers
2054222	New	Programmer	Category C	Trace data lost during collection stop in TRBE
2058367	New	Programmer	Category C	L3D_CACHE_ALLOC PMU inaccurate when using WriteEvictOrEvict transactions

December 08, 2020: Changes in document version v6.0

ID	Status	Area	Category	Summary
2008768	New	Programmer	Category B	RAS errors during core power down might cause a deadlock
2012097	New	Programmer	Category B	TRBE writes to MTE tagged pages might not report external aborts
2017096	New	Programmer	Category B	Streaming STG and STG2 performance lower than expected with TCF=NONE
2017087	New	Programmer	Category C	DSB might not guarantee completion of direct reads of L2 cache memories
2025108	New	Programmer	Category C	Corrupted register state results from executing specific form of SEL instruction followed by SVE AESMC or AESIMC instruction

November 06, 2020: Changes in document version v5.0

ID	Status	Area	Category	Summary
1791789	Updated	Programmer	Category A	Fault info captured in FAR and ESR registers for LDP 64-bit variant could be incorrect
1793423	Updated	Programmer	Category B	An unexpected data abort might occur under specific micro-architectural conditions following an abort on an earlier instruction
1887413	Updated	Programmer	Category B	Executing a SVE load with no active predicates might result in a deadlock under certain micro-architectural conditions
1901946	Updated	Programmer	Category B	Executing software prefetch instructions from a context with memory tagging enabled might lead to corruption of architecture state
1917258	Updated	Programmer	Category B	Non-fault SVE load does not update FFR when it reads data with ECC error or external abort
1984319	New	Programmer	Category B	Incorrect read value for Performance Monitors Common Event Identification Register
2002765	New	Programmer	Category B	Embedded Trace of WFI or WFE instructions might corrupt PE architectural state
1971496	New	Programmer	Category C	VMID value in trace packets might be incorrect
1975917	New	Programmer	Category C	AMU Event 0x0011, Core frequency cycles might increment incorrectly when the core is in WFI or WFE state
1980906	New	Programmer	Category C	Reset Catch debug event might not cause core to enter Debug state immediately after Cold reset
1986267	New	Programmer	Category C	DRPS might not execute correctly in Debug state with SCTLR_ELx.IESB set in the current EL
1989365	New	Programmer	Category C	Floating-point Operations speculatively executed PMU events are not counted
2000010	New	Programmer	Category C	Execution of STG instructions in close proximity might incorrectly write MTE Allocation Tag to memory more than once

September 30, 2020: Changes in document version v4.0

ID	Status	Area	Category	Summary
1927200	New	Programmer	Category B	Atomic instructions with acquire semantics might not be ordered with respect to older stores with release semantics
1920871	Updated	Programmer	Category C	MPAM value associated with translation table walk request might be incorrect
1938354	Updated	Programmer	Category C	Incorrect fault status code might be reported in Trace Buffer Extension register TRBSR_EL1.FSC
1911676	New	Programmer	Category C	TFSR contents might be incorrect after executing a page crossing SVE predicated load instruction
1949697	New	Programmer	Category C	A Checked store that crosses a page boundary might not perform a Tag Check

August 26, 2020: Changes in document version v3.0

ID	Status	Area	Category	Summary
1887102	New	Programmer	Category B	IPA based TLB invalidate might fail to invalidate translation table entries caching translations for the Trace Buffer Extension
1890822	New	Programmer	Category B	Stage 2 abort during Secure EL1 translation might report incorrect NS value in HPFAR_EL2
1901946	New	Programmer	Category B	Executing software prefetch instructions from a context with memory tagging enabled might lead to corruption of architecture state
1906301	New	Programmer	Category B	Core might deadlock when memory-mapped read to Debug/Trace/PMU register is followed by WFI or WFE
1914047	New	Programmer	Category B	External debugger access to Debug registers might not work during Warm reset
1916945	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
1917258	New	Programmer	Category B	Non-fault SVE load does not update FFR when it reads data with ECC error or external abort
1918765	New	Programmer	Category B	CFP RCTX and CPP RCTX instructions might incorrectly execute as a NOP in ELO
1934260	New	Programmer	Category B	Tag checked streaming write might report false fail
1851816	Updated	Programmer	Category C	The MPAM value associated with MMU descriptor fetch requests might be incorrect
1875555	New	Programmer	Category C	Compare and Swap (CAS) instructions with stack pointer as base register are incorrectly treated as checked accesses
1884880	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 page table entry which has been modified
1893664	New	Programmer	Category C	Accessing a memory location using mismatched shareability attributes when MTE tag checking is enabled might lose coherency or deadlock

ID	Status	Area	Category	Summary
1896171	New	Programmer	Category C	Access to External Debug Auxiliary Processor Feature Register might incorrectly return an error response
1899211	New	Programmer	Category C	Some corrected errors might incorrectly increment ERR0MISCO.CECC or ERR0MISCO.CECO
1899435	New	Programmer	Category C	PFG duplicate reported faults through a Warm reset
1909702	New	Programmer	Category C	IDATAN_EL3 might represent incorrect value after direct memory access to internal memory for Instruction TLB
1919240	New	Programmer	Category C	The PE might deadlock if Pseudofault Injection is enabled in Debug State
1920415	New	Programmer	Category C	Trace Buffer might write trace packets to memory using incorrect cache attributes
1920634	New	Programmer	Category C	A Checked store with poisoned tags might result in a Tag Check Fail instead of taking an SError interrupt exception
1920871	New	Programmer	Category C	MPAM value associated with translation table walk request might be incorrect
1925506	New	Programmer	Category C	Unsupported atomic fault due to memory type defined in first stage of translation might result in exception being taken to EL2
1926908	New	Programmer	Category C	Access with additional latency from alignment (LDST_ALIGN_LAT) PMU event does not count
1927566	New	Programmer	Category C	ERR0MISCO_EL1.SUBARRAY value for ECC errors in the L1 data cache might be incorrect
1929989	New	Programmer	Category C	Event Stream from the Virtual Counter is not correctly disabled by VHE in Secure State
1938354	New	Programmer	Category C	Incorrect fault status code might be reported in Trace Buffer Extension register TRBSR_EL1.FSC

June 25, 2020: Changes in document version v2.0

ID	Status	Area	Category	Summary
1791789	Updated	Programmer	Category A	Fault info captured in FAR and ESR registers for LDP 64-bit variant could be incorrect
1785648	Updated	Programmer	Category B	Atomic store instructions to shareable write-back memory might cause memory consistency failures
1793423	Updated	Programmer	Category B	An unexpected data abort might occur under specific micro-architectural conditions following an abort on an earlier instruction
1801992	Updated	Programmer	Category B	Hardware Access/Dirty flag updates might indicate successful completion, but PTE is not updated
1813969	Updated	Programmer	Category B	TLBI range instructions with NUM>31 may not invalidate all required entries+
1863568	New	Programmer	Category B	Core might generate Breakpoint exception on incorrect IA
1887413	New	Programmer	Category B	Executing a SVE load with no active predicates might result in a deadlock under certain micro-architectural conditions

ID	Status	Area	Category	Summary
1786338	Updated	Programmer	Category C	Memory uploads and downloads via memory access mode within Debug state can fail to accurately read or write memory contents
1787272	Updated	Programmer	Category C	TSB instruction completion can be delayed when executed in region where trace is allowed
1799975	Updated	Programmer	Category C	Watchpoint Exception on DC ZVA does not report correct address in FAR or EDWAR
1804175	Updated	Programmer	Category C	CTI event from the core to the external DebugBlock might be dropped
1804563	Updated	Programmer	Category C	Trace Buffer Extension unit might write trace packets to memory using incorrect memory page attributes
1817593	Updated	Programmer	Category C	Persistent faults on speculative elements of SVE First-fault gather-load instructions might result in deadlock
1827136	Updated	Programmer	Category C	External debug accesses in memory access mode with SCTLR_ELx.IESB set might result in unpredictable behavior
1838906	New	Programmer	Category C	Noncompliance with prioritization of Exception Catch debug events
1851171	New	Programmer	Category C	Transient L2 tag double bit Errors might cause data corruption
1851323	New	Programmer	Category C	Incorrect trace timestamp value when self-hosted trace is disabled
1851816	New	Programmer	Category C	The MPAM value associated with MMU descriptor fetch requests might be incorrect
1855551	New	Programmer	Category C	ERRORMISC0_EL1.SUBARRAY, ERROSTATUS.CE and ERROSTATUS.DE values for ECC errors in the L1 data cache might be incorrect
1859562	New	Programmer	Category C	Incorrect read value for the Trace ID Register 3 SYSSTALL field
1862651	New	Programmer	Category C	Incorrect read value for External Debug Processor Feature Register
1865453	New	Programmer	Category C	The values for fields ID_AA64ZFR0_EL1.{SM4,SHA3,AES} read incorrectly as non-zero
1868638	New	Programmer	Category C	The core does not treat the BAS field of the Debug Breakpoint Control Register as RES1
1870363	New	Programmer	Category C	L2 data RAM may fail to report corrected ECC errors
1875745	New	Programmer	Category C	A Checked load that fails a Tag Check could set the ESR to an incorrect value

May 12, 2020: Changes in document version v1.0

ID	Status	Area	Category	Summary
1791789	New	Programmer	Category A	Fault info captured in FAR and ESR registers for LDP 64-bit variant could be incorrect
1785648	New	Programmer	Category B	Atomic store instructions to shareable write-back memory might cause memory consistency failures
1793423	New	Programmer	Category B	An unexpected data abort might occur under specific micro-architectural conditions following an abort on an earlier instruction
1801992	New	Programmer	Category B	Hardware Access/Dirty flag updates might indicate successful completion, but PTE is not updated
1813969	New	Programmer	Category B	TLBI range instructions with NUM>31 may not invalidate all required entries+
1786338	New	Programmer	Category C	Memory uploads and downloads via memory access mode within Debug state can fail to accurately read or write memory contents
1787272	New	Programmer	Category C	TSB instruction completion can be delayed when executed in region where trace is allowed
1799975	New	Programmer	Category C	Watchpoint Exception on DC ZVA does not report correct address in FAR or EDWAR
1804175	New	Programmer	Category C	CTI event from the core to the external DebugBlock might be dropped
1804563	New	Programmer	Category C	Trace Buffer Extension unit might write trace packets to memory using incorrect memory page attributes
1817593	New	Programmer	Category C	Persistent faults on speculative elements of SVE First-fault gather-load instructions might result in deadlock
1827136	New	Programmer	Category C	External debug accesses in memory access mode with SCTLR_ELx.IESB set might result in unpredictable behavior

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
1791789	Programmer	Category A	Fault info captured in FAR and ESR registers for LDP 64-bit variant could be incorrect	r0p0, r1p0, r2p0	r2p1
1785648	Programmer	Category B	Atomic store instructions to shareable write-back memory might cause memory consistency failures	r0p0	r1p0
1793423	Programmer	Category B	An unexpected data abort might occur under specific micro-architectural conditions following an abort on an earlier instruction	r0p0	r1p0
1801992	Programmer	Category B	Hardware Access/Dirty flag updates might indicate successful completion, but PTE is not updated	r0p0	r1p0
1813969	Programmer	Category B	TLBI range instructions with NUM>31 may not invalidate all required entries+	r0p0	r1p0
1863568	Programmer	Category B	Core might generate Breakpoint exception on incorrect IA	r0p0	r1p0
1887102	Programmer	Category B	IPA based TLB invalidate might fail to invalidate translation table entries caching translations for the Trace Buffer Extension	r0p0, r1p0	r2p0
1887413	Programmer	Category B	Executing a SVE load with no active predicates might result in a deadlock under certain micro-architectural conditions	r0p0	r1p0
1890822	Programmer	Category B	Stage 2 abort during Secure EL1 translation might report incorrect NS value in HPFAR_EL2	r0p0, r1p0	r2p0
1901946	Programmer	Category B	Executing software prefetch instructions from a context with memory tagging enabled might lead to corruption of architecture state	r1p0	r2p0
1906301	Programmer	Category B	Core might deadlock when memory-mapped read to Debug/Trace/PMU register is followed by WFI or WFE	r0p0, r1p0	r2p0
1914047	Programmer	Category B	External debugger access to Debug registers might not work during Warm reset	r0p0, r1p0	r2p0

ID	Area	Category	Summary	Found in versions	Fixed in version
1916945	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, r1p0	r2p0
1917258	Programmer	Category B	Non-fault SVE load does not update FFR when it reads data with ECC error or external abort	r0p0, r1p0	r2p0
1918765	Programmer	Category B	CFP RCTX and CPP RCTX instructions might incorrectly execute as a NOP in ELO	r0p0, r1p0	r2p0
1927200	Programmer	Category B	Atomic instructions with acquire semantics might not be ordered with respect to older stores with release semantics	r0p0, r1p0	r2p0
1934260	Programmer	Category B	Tag checked streaming write might report false fail	r1p0	r2p0
1984319	Programmer	Category B	Incorrect read value for Performance Monitors Common Event Identification Register	r0p0, r1p0, r2p0	r2p1
2002765	Programmer	Category B	Embedded Trace of WFI or WFE instructions might corrupt PE architectural state	r0p0, r1p0, r2p0	r2p1
2008768	Programmer	Category B	RAS errors during core power down might cause a deadlock	r0p0, r1p0, r2p0	r2p1
2012097	Programmer	Category B	TRBE writes to MTE tagged pages might not report external aborts	r1p0, r2p0	r2p1
2017096	Programmer	Category B	Streaming STG and STG2 performance lower than expected with TCF=NONE	r0p0, r1p0, r2p0	r2p1
2023111	Programmer	Category B	Utility Bus register accesses to reserved addresses of PE might hang	r0p0, r1p0, r2p0	r2p1
2054223	Programmer	Category B	The trace data is not flushed completely during a TSB instruction executed in prohibited region	r0p0, r1p0, r2p0	r2p1
2058056	Programmer	Category B	Disabling of data prefetcher with outstanding prefetch TLB miss might cause a deadlock	r0p0, r1p0, r2p0, r2p1	Open
2081180	Programmer	Category B	Executing a WFI or WFE instruction after a STREX instruction might result in a deadlock under specific conditions	r0p0, r1p0, r2p0	r2p1
2083908	Programmer	Category B	Execution of ST2G instructions in close proximity might cause loss of MTE allocation tag data	r2p0	r2p1

ID	Area	Category	Summary	Found in versions	Fixed in version
2119858	Programmer	Category B	Trace data might get overwritten in TRBE FILL mode	r0p0, r1p0, r2p0	r2p1
2136059	Programmer	Category B	The CPP instruction will apply to an incorrect EL context	r0p0, r1p0, r2p0	r2p1
2147715	Programmer	Category B	A CFP instruction might not invalidate the correct resources	r2p0	r2p1
2216384	Programmer	Category B	PDP deadlock due to CMP/CMN + B.AL/B.NV fusion	r0p0, r1p0, r2p0	r2p1
2219376	Programmer	Category B	Enabling TRBE might cause a data write to a page with the wrong ASID when owning Exception level is EL1	r0p0, r1p0, r2p0	r2p1
2224489	Programmer	Category B	TRBE might cause a data write to an out-of-range address which is not reserved for TRBE	r0p0, r1p0, r2p0	r2p1
2267065	Programmer	Category B	A CFP instruction might execute with incorrect upper ASID or VMID bits	r0p0, r1p0, r2p0	r2p1
2282622	Programmer	Category B	Continuous failing STREX because of another PE executing prefetch for store behind consistently mispredicted branch	r0p0, r1p0, r2p0, r2p1	Open
2291219	Programmer	Category B	Denied power down request might prevent completion of future power down request	r0p0, r1p0, r2p0	r2p1
2371105	Programmer	Category B	Translation table walk folding into an L1 prefetch might cause data corruption	r0p0, r1p0, r2p0	r2p1
2381390	Programmer	Category B	A continuous stream of incoming DVM syncs may cause TRBE to prevent the CPU from forward progressing	r0p0, r1p0, r2p0	r2p1
2701952	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, r1p0, r2p0, r2p1	Open
2742423	Programmer	Category B	Page crossing access that generates an MMU fault on the second page could result in a livelock	r0p0, r1p0, r2p0, r2p1	Open
2768515	Programmer	Category B	The core might deadlock during powerdown sequence	r0p0, r1p0, r2p0, r2p1	Open
2778471	Programmer	Category B	The PE might generate memory accesses using invalidated mappings after completion of a DVM SYNC operation	r0p0, r1p0, r2p0, r2p1	Open

ID	Area	Category	Summary	Found in versions	Fixed in version
3003018	Programmer	Category B	PE executing DRPS during Debug Halt under Double Fault condition will not execute properly	r0p0, r1p0, r2p0, r2p1	Open
3038569	Programmer	Category B	TRBE might write to pages which lack write permission at Stage-1 or Stage-2	r0p0, r1p0, r2p0	r2p1
3099212	Programmer	Category B	PE might execute instructions consistent with previous context-synchronized state when SCR_EL3.EEL2 is changed	r0p0, r1p0, r2p0, r2p1	Open
2982956	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, r1p0, r2p0, r2p1	Open
1786338	Programmer	Category C	Memory uploads and downloads via memory access mode within Debug state can fail to accurately read or write memory contents	r0p0	r1p0
1787272	Programmer	Category C	TSB instruction completion can be delayed when executed in region where trace is allowed	r0p0	r1p0
1799975	Programmer	Category C	Watchpoint Exception on DC ZVA does not report correct address in FAR or EDWAR	r0p0	r1p0
1804175	Programmer	Category C	CTI event from the core to the external DebugBlock might be dropped	r0p0	r1p0
1804563	Programmer	Category C	Trace Buffer Extension unit might write trace packets to memory using incorrect memory page attributes	r0p0	r1p0
1817593	Programmer	Category C	Persistent faults on speculative elements of SVE First-fault gather-load instructions might result in deadlock	r0p0	r1p0
1827136	Programmer	Category C	External debug accesses in memory access mode with SCTLR_ELx.IESB set might result in unpredictable behavior	r0p0	r1p0
1838906	Programmer	Category C	Noncompliance with prioritization of Exception Catch debug events	r0p0, r1p0, r2p0, r2p1	Open
1851171	Programmer	Category C	Transient L2 tag double bit Errors might cause data corruption	r0p0	r1p0
1851323	Programmer	Category C	Incorrect trace timestamp value when self-hosted trace is disabled	r0p0	r1p0

ID	Area	Category	Summary	Found in versions	Fixed in version
1851816	Programmer	Category C	The MPAM value associated with MMU descriptor fetch requests might be incorrect	r0p0, r1p0	r2p0
1855551	Programmer	Category C	ERR0MISCO_EL1.SUBARRAY, ERR0STATUS.CE and ERR0STATUS.DE values for ECC errors in the L1 data cache might be incorrect	r0p0	r1p0
1859562	Programmer	Category C	Incorrect read value for the Trace ID Register 3 SYSSTALL field	r0p0	r1p0
1862651	Programmer	Category C	Incorrect read value for External Debug Processor Feature Register	r0p0	r1p0
1865453	Programmer	Category C	The values for fields ID_AA64ZFR0_EL1.{SM4,SHA3,AES} read incorrectly as non-zero	r0p0	r1p0
1868638	Programmer	Category C	The core does not treat the BAS field of the Debug Breakpoint Control Register as RES1	r0p0	r1p0
1870363	Programmer	Category C	L2 data RAM may fail to report corrected ECC errors	r0p0	r1p0
1875555	Programmer	Category C	Compare and Swap (CAS) instructions with stack pointer as base register are incorrectly treated as checked accesses	r1p0	r2p0
1875745	Programmer	Category C	A Checked load that fails a Tag Check could set the ESR to an incorrect value	r1p0	r2p0
1884880	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 page table entry which has been modified	r0p0, r1p0, r2p0, r2p1	Open
1893664	Programmer	Category C	Accessing a memory location using mismatched shareability attributes when MTE tag checking is enabled might lose coherency or deadlock	r1p0	r2p0
1896171	Programmer	Category C	Access to External Debug Auxiliary Processor Feature Register might incorrectly return an error response	r0p0, r1p0	r2p0
1899211	Programmer	Category C	Some corrected errors might incorrectly increment ERR0MISCO.CECC or ERR0MISCO.CECO	r0p0, r1p0, r2p0	r2p1
1899435	Programmer	Category C	PFG duplicate reported faults through a Warm reset	r0p0, r1p0	r2p0

ID	Area	Category	Summary	Found in versions	Fixed in version
1909702	Programmer	Category C	IDATAn_EL3 might represent incorrect value after direct memory access to internal memory for Instruction TLB	r0p0, r1p0, r2p0, r2p1	Open
1911676	Programmer	Category C	TFSR contents might be incorrect after executing a page crossing SVE predicated load instruction	r1p0, r2p0	r2p1
1919240	Programmer	Category C	The PE might deadlock if Pseudofault Injection is enabled in Debug State	r0p0, r1p0	r2p0
1920415	Programmer	Category C	Trace Buffer might write trace packets to memory using incorrect cache attributes	r0p0, r1p0	r2p0
1920634	Programmer	Category C	A Checked store with poisoned tags might result in a Tag Check Fail instead of taking an SError interrupt exception	r1p0	r2p0
1920871	Programmer	Category C	MPAM value associated with translation table walk request might be incorrect	r0p0, r1p0, r2p0	r2p1
1925506	Programmer	Category C	Unsupported atomic fault due to memory type defined in first stage of translation might result in exception being taken to EL2	r0p0, r1p0	r2p0
1926908	Programmer	Category C	Access with additional latency from alignment (LDST_ALIGN_LAT) PMU event does not count	r0p0, r1p0	r2p0
1927566	Programmer	Category C	ERRORMISCO_EL1.SUBARRAY value for ECC errors in the L1 data cache might be incorrect	r0p0, r1p0	r2p0
1929989	Programmer	Category C	Event Stream from the Virtual Counter is not correctly disabled by VHE in Secure State	r0p0, r1p0	r2p0
1938354	Programmer	Category C	Incorrect fault status code might be reported in Trace Buffer Extension register TRBSR_EL1.FSC	r0p0, r1p0, r2p0	r2p1
1949697	Programmer	Category C	A Checked store that crosses a page boundary might not perform a Tag Check	r1p0, r2p0	r2p1
1971496	Programmer	Category C	VMID value in trace packets might be incorrect	r0p0, r1p0, r2p0	r2p1
1975917	Programmer	Category C	AMU Event 0x0011, Core frequency cycles might increment incorrectly when the core is in WFI or WFE state	r0p0, r1p0, r2p0, r2p1	Open

ID	Area	Category	Summary	Found in versions	Fixed in version
1980906	Programmer	Category C	Reset Catch debug event might not cause core to enter Debug state immediately after Cold reset	r0p0, r1p0, r2p0	r2p1
1986267	Programmer	Category C	DRPS might not execute correctly in Debug state with SCTLR_ELx.IESB set in the current EL	r0p0, r1p0, r2p0	r2p1
1989365	Programmer	Category C	Floating-point Operations speculatively executed PMU events are not counted	r0p0, r1p0, r2p0	r2p1
2000010	Programmer	Category C	Execution of STG instructions in close proximity might incorrectly write MTE Allocation Tag to memory more than once	r2p0	r2p1
2002779	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, r1p0, r2p0	r2p1
2017087	Programmer	Category C	DSB might not guarantee completion of direct reads of L2 cache memories	r0p0, r1p0, r2p0	r2p1
2018317	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, r1p0, r2p0	r2p1
2025108	Programmer	Category C	Corrupted register state results from executing specific form of SEL instruction followed by SVE AESMC or AESIMC instruction	r0p0, r1p0, r2p0	r2p1
2050953	Programmer	Category C	External aborts for streaming writes to MTE tagged pages may report multiple errors	r1p0, r2p0	r2p1
2052424	Programmer	Category C	An execution of MSR instruction might not update the destination register correctly when an external debugger initiates APB write operation to update debug registers	r0p0, r1p0, r2p0	r2p1
2054222	Programmer	Category C	Trace data lost during collection stop in TRBE	r0p0, r1p0, r2p0	r2p1
2058367	Programmer	Category C	L3D_CACHE_ALLOC PMU inaccurate when using WriteEvictOrEvict transactions	r0p0, r1p0, r2p0	r2p1
2058540	Programmer	Category C	Incorrect Fault Status code reported for predicated SVE op	r0p0, r1p0, r2p0	r2p1
2061107	Programmer	Category C	Tag check fail might not be reported for an unaligned predicated SVE store	r0p0, r1p0, r2p0	r2p1

ID	Area	Category	Summary	Found in versions	Fixed in version
2089668	Programmer	Category C	OSECRR_EL1/EDECCR is incorrectly included in the Warm Reset domain	r0p0, r1p0, r2p0	r2p1
2093019	Programmer	Category C	Extra A-sync packet might get written to Trace Buffer in Trace prohibited region	r0p0, r1p0, r2p0	r2p1
2109742	Programmer	Category C	Speculative access to a recently unmapped physical address previously containing page tables might occur	r0p0, r1p0, r2p0	r2p1
2112535	Programmer	Category C	L1D_CACHE_INVALID and L2D_CACHE_INVALID PMU events fail to increment for SnpPreferUnique and SnpPreferUniqueFwd	r0p0, r1p0, r2p0	r2p1
2113481	Programmer	Category C	MPAM value associated with instruction fetch might be incorrect	r0p0, r1p0, r2p0, r2p1	Open
2117983	Programmer	Category C	Data abort on SVE first fault load might be routed to incorrect Exception level	r1p0, r2p0	r2p1
2141645	Programmer	Category C	A64 WFI or A64 WFE executed in Debug state suspends execution indefinitely	r0p0, r1p0, r2p0	r2p1
2143136	Programmer	Category C	Some SVE PMU events count incorrectly	r0p0, r1p0, r2p0	r2p1
2146514	Programmer	Category C	PMU Event MEM_ACCESS_CHECKED_WR, 0x4026 counts incorrectly and MEM_ACC_CHECKED 0x4024 might be incorrect	r1p0, r2p0	r2p1
2154216	Programmer	Category C	FAR_ELx contents for a Data Abort exception on SVE first fault contiguous load instruction due to Tag Check fail might be incorrect	r0p0, r1p0, r2p0	r2p1
2159150	Programmer	Category C	Direct access of L2 data RAMs using RAMINDEX returns incomplete data	r0p0, r1p0, r2p0	r2p1
2174188	Programmer	Category C	PMU_HOVFS event not always exported when self-hosted trace is disabled	r0p0, r1p0, r2p0	r2p1
2178034	Programmer	Category C	An SError might not be reported for an atomic store that encounters data poison	r0p0, r1p0, r2p0	r2p1
2186347	Programmer	Category C	64 bit source SVE PMULLB/T not considered Cryptography instruction	r0p0, r1p0, r2p0	r2p1

ID	Area	Category	Summary	Found in versions	Fixed in version
2227174	Programmer	Category C	Streaming writes to memory mapped Non-shareable and write-back might cause data corruption because of reordering	r0p0, r1p0, r2p0	r2p1
2238108	Programmer	Category C	Read or write from Secure EL1 for ICV_BPR1_EL1 register might not work	r0p0, r1p0, r2p0	r2p1
2238111	Programmer	Category C	Reads of DISR_EL1 incorrectly return 0s while in Debug State	r0p0, r1p0, r2p0	r2p1
2239139	Programmer	Category C	DRPS instruction is not treated as UNDEFINED at ELO in Debug state	r0p0, r1p0, r2p0	r2p1
2243871	Programmer	Category C	ELR_ELx[63:48] might hold incorrect value when PE disables address translation	r0p0, r1p0, r2p0	r2p1
2245716	Programmer	Category C	TRBE might use incorrect Cacheability attributes for TRBE data when address translation is disabled	r0p0, r1p0, r2p0	r2p1
2245832	Programmer	Category C	ESR_ELx contents for a Data Abort exception might be incorrect when an L1D tag double bit error is encountered	r0p0, r1p0, r2p0	r2p1
2247178	Programmer	Category C	L1 MTE Tag poison is not cleared	r1p0, r2p0	r2p1
2254450	Programmer	Category C	L1 Data poison is not cleared by a store	r0p0, r1p0, r2p0	r2p1
2276444	Programmer	Category C	PMU event for full/partial/empty predicate incorrect for some SVE instructions	r0p0, r1p0, r2p0	r2p1
2278134	Programmer	Category C	PMU L1D_CACHE_REFILL_OUTER is inaccurate	r0p0, r1p0, r2p0	r2p1
2283666	Programmer	Category C	Lower priority exception might be reported when abort condition is detected at both stages of translation	r0p0, r1p0, r2p0	r2p1
2307829	Programmer	Category C	ESR_ELx.ISV can be set incorrectly for an external abort on translation table walk	r0p0, r1p0, r2p0	r2p1
2317617	Programmer	Category C	ESR_ELx contents for a Data Abort exception might be incorrect when a data double bit error or external abort is encountered	r0p0, r1p0, r2p0	r2p1
2334390	Programmer	Category C	L2 tag RAM double-bit ECC error might lead to the PE not responding to a forwarding snoop	r0p0, r1p0, r2p0	r2p1

ID	Area	Category	Summary	Found in versions	Fixed in version
2344960	Programmer	Category C	CSSELR_EL1.TnD is RAZ/WI when CSSELR_EL1.InD == 0x1	r0p0, r1p0, r2p0	r2p1
2382765	Programmer	Category C	Incorrect read value for Performance Monitors Configuration Register	r0p0, r1p0, r2p0	r2p1
2391680	Programmer	Category C	Software-step not done after exit from Debug state with an illegal value in DSPSR	r0p0, r1p0, r2p0, r2p1	Open
2444421	Programmer	Category C	PMU STALL_SLOT_BACKEND and STALL_SLOT_FRONTEND events count incorrectly	r0p0, r1p0, r2p0, r2p1	Open
2643627	Programmer	Category C	ERXPFGCDN_EL1 register is incorrectly written on Warm reset	r0p0, r1p0, r2p0, r2p1	Open
2647274	Programmer	Category C	Incorrect read value for Performance Monitors Control Register	r0p0, r1p0, r2p0, r2p1	Open
2652240	Programmer	Category C	FAR_ELx contents for a Data Abort exception on SVE first fault contiguous load instruction due to Tag Check fail might be incorrect	r0p0, r1p0, r2p0, r2p1	Open
2676362	Programmer	Category C	Execution of STG instructions in close proximity might cause loss of MTE allocation tag data	r1p0, r2p0, r2p1	Open
2692441	Programmer	Category C	L3D PMU events may be inaccurate	r0p0, r1p0, r2p0, r2p1	Open
2694769	Programmer	Category C	MTE checked load might read an old value of allocation tag by not complying with address dependency ordering	r1p0, r2p0, r2p1	Open
2712632	Programmer	Category C	Incorrect read value for Performance Monitors Configuration Register EX field	r0p0, r1p0, r2p0, r2p1	Open
2726256	Programmer	Category C	IRG instructions might produce the wrong tag when GCR_EL1.RRND=0x0	r0p0, r1p0, r2p0, r2p1	Open
2769023	Programmer	Category C	STALL_BACKEND_MEM, Memory stall cycles AMU event count incorrectly	r0p0, r1p0, r2p0, r2p1	Open
2798805	Programmer	Category C	Incorrect decoding of SVE version of PRF* scalar plus scalar instructions	r0p0, r1p0, r2p0, r2p1	Open
2799687	Programmer	Category C	ECC errors in MTE allocation tags may lead to silent data corruption in tag values	r1p0, r2p0, r2p1	Open

ID	Area	Category	Summary	Found in versions	Fixed in version
2814414	Programmer	Category C	Incorrect timestamp value reported in SPE records when timestamp capture is enabled	r0p0, r1p0, r2p0, r2p1	Open
2814418	Programmer	Category C	PE may fail to detect multiple uncorrectable ECC errors in the L1 data cache tag RAM	r0p0, r1p0, r2p0, r2p1	Open
2817889	Programmer	Category C	TRBE buffer write translation out of context may have incorrect memory attributes	r0p0, r1p0, r2p0, r2p1	Open
2910963	Programmer	Category C	L2D_CACHE_WB_CLEAN overcounts	r0p0, r1p0, r2p0, r2p1	Open
2921487	Programmer	Category C	Accessing a memory location using mismatched Shareability attributes when MTE tag checking is enabled might cause data corruption	r0p0, r1p0, r2p0, r2p1	Open
3061569	Programmer	Category C	TagMatch responses with error indication do not generate a SError abort	r0p0, r1p0, r2p0, r2p1	Open

Errata descriptions

Category A

1791789

Fault info captured in FAR and ESR registers for LDP 64-bit variant might be incorrect

Status

Fault Type: Programmer Category A

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

Under certain conditions, the FAR (Fault Address Register) and ESR (Exception Syndrome Register) might have incorrect values when the LDP (Load Pair) 64-bit variant generates an abort.

Configurations affected

All configurations are affected.

Conditions

All of the following conditions must be met:

1. The LDP 64-bit variant crosses a page boundary.
2. Data read from lower bytes on the first page results in a synchronous abort due to an internal ECC error, external abort, or MTE tag check fail.
3. Data read from upper bytes on the second page results in alignment fault, MMU fault, or watchpoint exception.

Implications

If the above conditions are met, the contents of the FAR and ESR registers might have incorrect values.

Workaround

This erratum can be avoided by setting CPUACTLR5_EL1[10] to 1. Setting CPUACTLR5_EL1[10] to 1 would have a significant performance (approximately 20%) impact on streaming workloads that use the LDP 64-bit variant. Performance impact on non-streaming workloads would be much smaller (approximately 1%).

Category A (rare)

There are no errata in this category.

Category B

1785648

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 r1p0.

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 that include a DSU L3 cache or Snoop Filter, or have an interconnect capable of handling far atomic transactions indicated by the BROADCASTATOMIC pin being set to 1.

Conditions

1. PEO executes atomic store instruction that hits in the L1 data cache and L2 cache in the Shared state.
2. PEO 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. PEO invalidating snoop to the L1 data cache is delayed due to internal queueing.

Implications

If the above conditions are met, PEO 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.

1793423

An unexpected data abort might occur under specific micro-architectural conditions following an abort on an earlier instruction

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0. Fixed in r1p0.

Description

Under certain micro-architectural conditions, an abort on a LDP 64-bit variant could leave the processor in a state that allows a subsequent instruction to report an unexpected data abort.

Configurations affected

All configurations are affected.

Conditions

All of the following conditions must be met:

1. LDP 64-bit variant signals a data abort.
2. An Instruction accessing memory is issued after the core services the LDP 64-bit variant data abort.

Implications

If the above conditions are met under specific micro-architectural conditions, the core might report an unexpected data abort after it services the data abort for LDP 64-bit variant.

Workaround

This erratum can be avoided by setting CPUACTLR5_EL1[10] to 1. Setting CPUACTLR5_EL1[10] to 1 will have a performance impact on workloads that use LDP 64-bit variant.

1801992

Hardware Access/Dirty flag updates might indicate successful completion, but PTE is not updated

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0. Fixed in r1p0.

Description

A page table walk that causes a hardware update of the Access or Dirty flags of the PTE (Page Table Entry) and requires an external request on the CHI interface, might indicate success to the MMU when the PTE Access and Dirty flags are not updated.

Configurations affected

All configurations are affected.

Conditions

1. Error detection and correction within the PE caches is disabled by `ERROCTLR.ED=0`.
2. MMU page table walk causes a hardware update of Access or Dirty flags in the PTE.
3. A/D update operation hits in the L2 cache on a line in a shared state, and issues a `MakeReadUnique` transaction.
4. Critical data beat returns without error indication is forwarded to the MMU, which allows the A/D update to succeed.
5. One or more subsequent data beats for the same cache line receives an error response.

Implications

If the above conditions are met, data returned to the MMU by the A/D update might indicate success, while the PTE cached by the L2 cache is not updated because the errors in the non-critical data beats could not be deferred. This might lead to successful performance of a load or store that should have taken an abort.

Workaround

If error detection and correction within the PE caches is disabled by `ERROCTLR.ED=0`, then set `CPUACTLR2_EL1[43]` to disable forwarding of the critical data beat.

1813969

TLBI range instructions with NUM>31 may not invalidate all required entries+

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0. Fixed in r1p0.

Description

When executing a TLB Invalidate (TLBI) range operation, if the NUM field of the operand has a value of 32 or higher, then the PE TLBs may not invalidate all the required entries. In addition, a TLBI DVM message might not convey the correct NUM value.

Configurations affected

This erratum affects all configurations.

Conditions

1. PE executes a TLBI range operation with a NUM argument of 32 or larger.

Implications

If the above conditions are met, the PE TLB might not invalidate all the required entries and a TLBI DVMMsg broadcast might not convey the correct NUM value.

Workaround

Software should not use TLBI range operations and use non-range TLBI operations instead.

1863568

Core might generate Breakpoint exception on incorrect IA

Status

Fault Type: Programmer Category B
Fault Status: Present in r0p0. Fixed in r1p0.

Description

Under certain conditions, the core can generate a breakpoint exception on the instruction sequentially before the address specified in the Debug Breakpoint Value Register (DBGBVR).

Configurations Affected

This erratum affects all configurations.

Conditions

1. Hardware breakpoint is enabled.

Implications

If the above conditions are met, breakpoint exception will incorrectly occur on the instruction sequentially before the hardware breakpoint address specified.

Workaround

Set CPUACTLR_EL1[21] to 1. Setting this bit does not affect performance unless breakpoints are in use.

1887102

IPA based TLB Invalidate might fail to invalidate translation table entries caching translations for the Trace Buffer Extension

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

Description

When the Trace Buffer Extension (TBRE) is enabled and TRBLIMITR_EL1.nVM is set, addresses generated by the TBRE are considered Intermediate Physical Addresses (IPA). Under such a scenario, a TLB Invalidate by IPA operation (TLBIIPAS2IS) might fail to invalidate translation table entries accessible to the TBRE.

Configurations affected

This erratum affects all configurations.

Conditions

1. PEO TRBE is enabled.
2. PEO TRBLIMITR_EL1.nVM bit is set.
3. PE1 executes an Inner Shareable TLBI by IPA and a DSB which are snooped by PEO.
4. PE1 does not execute an Inner Shareable TLBI by VA or TLBI by VMID before the DSB mentioned in condition 3.

Implications

If the above conditions occur, the TBRE might not invalidate its translation table entries and generate trace packets using an incorrect physical address.

Workaround

To avoid this erratum, software should:

- set CPUACTLR2[27] to 1 (to allow the injected DSB to invalidate translation table entries caching translations for TRBE), or
- execute Inner Shareable TLBI by VA or TLBI by VMID before the DSB.

1887413

Executing a SVE load with no active predicates might result in a deadlock under certain micro-architectural conditions

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0. Fixed in r1p0.

Description

Under certain micro-architectural conditions, executing a SVE load where all predicates are inactive might result in a deadlock

Configurations Affected

All configurations are affected.

Conditions

1. A predicated SVE load with no active lanes.

Implications

If the above conditions are met under specific micro-architectural conditions, the core might deadlock.

Workaround

This erratum can be avoided by setting CPUACTLR5_EL1[10] to 1. Setting CPUACTLR5_EL1[10] to 1 will impact performance on AArch64 code.

1890822

Stage 2 abort during Secure EL1 translation might report incorrect NS value in HPFAR_EL2

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

Description

Under certain conditions, a stage 2 permission or unsupported atomic fault generated on the translation table walk of Secure EL1 stage 1 translation might result in an incorrect value captured in the Non-Secure (NS) bit of HPFAR_EL2.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Stage 2 translation is enabled for Secure EL1.
2. Permission fault or unsupported atomic fault is generated in the second stage of translation performed during the translation table walk of Secure EL1 stage 1 translation.

Implications

If the above conditions are met, the NS bit value in the HPFAR_EL2 register might be incorrect. In this situation, which can be identified by the ESR_EL2 encoding, the Hypervisor running at Secure EL2 cannot rely on the NS field in the HPFAR_EL2 register. If it needs this information (as might be the case for a copy-on-write management of the memory holding stage 1 translation tables), it must determine it by some other means.

Workaround

There is no workaround.

1901946

Executing software prefetch instructions from a context with memory tagging enabled might lead to corruption of architecture state

Status

Fault Type: Programmer Category B

Fault Status: Present in r1p0. Fixed in r2p0.

Description

Under certain conditions, executing software prefetch instructions from a context with memory tagging enabled that accesses bytes from both Normal and Device memory could lead to corruption of architecture state.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Contiguous or gather variants of PRFD, PRFH, PRFW instructions are executed from a context.
2. Memory tagging is enabled for that context.
3. The prefetch instruction accesses bytes from both Normal and Device memory.

Implications

If the above conditions are met, architecture state might be corrupted.

Workaround

This erratum can be avoided by setting CPUACTLR4_EL1[15] to 1. Setting CPUACTLR4_EL1[15] to 1 will have a small impact on performance.

1906301

Core might deadlock when memory-mapped read to Debug/Trace/PMU register is followed by WFI or WFE

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

Description

When a load to device memory targeting a memory mapped component, such as Debug, Trace, or PMU register implemented on the same core is executed and is followed by a WFI/WFE instruction before the load data is returned to core, then it might deadlock the core.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Load to device memory targeting same core's memory mapped debug interface is executed.
2. WFI or WFE is executed in quick succession before the load instruction completes.

Implications

If the above conditions are met, then under certain conditions core might deadlock.

Workaround

Software should insert a DSB instruction between the load instruction and WFI/WFE instruction. This will ensure the load instruction completes before WFI/WFE is executed.

1914047

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

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

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.

Warm reset is asserted when the core is in the OFF_EMU, WARM_RST, or DBG_RECOV power modes.

Workaround

There is no workaround.

1916945

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, r1p0. Fixed in r2p0.

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 might 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.

1917258

Non-fault SVE load does not update FFR when it reads data with ECC error or external abort

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

Description

Under certain conditions, a Non-fault SVE load that reads data with double bit ECC error or external abort does not update FFR.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Non-fault SVE load makes data access.
2. Data access encounters double bit ECC error or external abort.

Implications

If the above conditions are met, FFR contents would be incorrect.

Workaround

This erratum can be avoided by setting CPUACTLR4_EL1[43] to 1. There is no performance impact associated with setting this bit.

1918765

CFP RCTX and CPP RCTX instructions might incorrectly execute as a NOP in ELO

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0. Fixed in r2p0..

Description

HCR_EL2.<E2H,TGE> and SCTLR_EL1.EnRCTX control the execution of CPP and CFP instructions in ELO. These instructions might incorrectly execute as a NOP instruction due to this erratum.

Configurations Affected

This erratum affects all configurations.

Conditions

1. SCTLR_EL1.EnRCTX=1 and E2H,TGE=(1,1)
2. CFP RCTX or CPP RCTX is executed at ELO

Implications

CFP RCTX and CPP RCTX instructions will be incorrectly executed as a NOP instruction.

Workaround

CFP RCTX and CPP RCTX can be trapped at ELO by setting SCTLR_EL2.EnRCTX=0 when E2H,TGE=1,1.

1927200

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, r1p0. Fixed in r2p0.

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, memory ordering violation might happen.

Workaround

This workaround assumes that MTE is not enabled in precise mode.

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

1934260

Tag checked streaming write might report false fail

Status

Fault Type: Programmer Category B
Fault Status: Present in r1p0. Fixed in r2p0.

Description

A PE performing tag-checked sequential writes that stream beyond the L1 data cache and hit in the L2 cache, might use stale allocation tags in the tag check comparison.

Configurations Affected

This erratum affects all configurations.

Conditions:

1. MTE is enabled in imprecise exception mode.
2. PE performs a write of allocation tags to cache line A.
3. PE performs writes to several contiguous cache lines such that write streaming mode is engaged.
4. Streaming write request to cache line A hits in L2 cache on a line present in the L1 data cache, and therefore must snoop the L1 data cache for possibly dirty allocation tags.
5. L1 data cache returns dirty allocation tags for cache line A.

Implications

If the above conditions are met, the L2 cache might use the stale tags from the L2 cache for the tag check comparison, which might lead to a false tag check fail, or a false tag check pass.

Workaround

When testing MTE software in imprecise mode, disable write streaming by setting CPUECTLR_EL1[25:18] to 'hff'. This workaround will result in reduced performance for workloads that benefit from write streaming.

When testing performance in MTE imprecise mode, no workaround is necessary. However, false MTE tag check fails might be reported to TFSR_ELx.

1984319

Incorrect read value for Performance Monitors Common Event Identification register

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

The AArch64 System register Performance Monitors Common Event Identification register 0 (PMCEID0_ELO) returns an incorrect read value for the following fields in the register:

- ID44
- ID48
- ID49
- ID50
- ID51
- ID56
- ID57
- ID58
- ID59

The external register Performance Monitors Common Event Identification register 2 (PMCEID2) returns an incorrect read value for the following fields in the register:

- ID12
- ID16
- ID17
- ID18
- ID19
- ID24
- ID25
- ID26
- ID27

Configurations Affected

All configurations are affected.

Conditions

- Software reads the AArch64 System register PMCEID0_ELO.
or

- Debugger reads the PMCEID2 register.

Implications

The register fields incorrectly report the value 0b0 indicating that the corresponding PMU common events are not implemented, or not counted. The expected value should be 0b1, as the corresponding PMU common events are implemented.

Workaround

Software can read the MIDR_EL1 register to identify the implemented PMU events.

2002765

Embedded Trace of WFI or WFE instructions might corrupt PE architectural state

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, and r2p0. Fixed in r2p1.

Description

Executing a **WFI** or **WFE** instruction with Embedded Trace enabled might corrupt AArch64 PSTATE.BTYPE or trace information intended for Embedded Trace, resulting in architecture violations.

Configurations Affected

This erratum affects all configurations.

Conditions

The erratum occurs under the following conditions:

1. Embedded Trace is enabled.
2. A **WFI** or **WFE** instruction is executed.

Implications

Under certain internal timing conditions exacerbated by a high frequency of branch instructions, the PE might corrupt PSTATE.BTYPE or trace information. Corruption of any of these values might lead to any of the following architecture violations:

- Applying erroneous BTYPE information to AArch64 instructions in guarded pages (wrong BTYPE value resulting in erroneous Branch Target Exceptions or failing to report a Branch Target Exception).
- Reporting erroneous trace information to Embedded Trace.

Workaround

This erratum can be worked around by using the instruction patching mechanism. This can be done through the following write sequence to several IMPLEMENTATION DEFINED registers. The code sequence should be applied early in the boot sequence prior to any of the possible errata conditions being met. There is no performance or power impact associated with this workaround.

```
LDR x0,=0x6
MSR S3_6_c15_c8_0,x0 ; MSR CPUPSELR_EL3, X0
LDR x0,=0xF3A08002
MSR S3_6_c15_c8_2,x0 ; MSR CPUPOR_EL3, X0
LDR x0,=0xFFF0F7FE
MSR S3_6_c15_c8_3,x0 ; MSR CPUPMR_EL3, X0
LDR x0,=0x40000001003ff
MSR S3_6_c15_c8_1,x0 ; MSR CPUPCR_EL3, X0
ISB
```

2008768

RAS errors during core power down might cause a deadlock

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

If a Reliability, Availability, and Serviceability (RAS) error occurs when a core is being powered down, then the power down sequence is designed to be aborted so that the error can be handled by software. As explained in this erratum, the power down sequence might complete despite the error occurring, or it might cause a deadlock.

Configurations affected

All configurations are affected.

Conditions

1. The ERXCTLR_EL1.ED bit is set for any of the core error records, and at least one of the CI, DUI, CFI, FI, or UI bits is set.
2. Software running on the core sets the CPUPWRCTLR.CORE_PWRDN_EN bit and executes a **WFI** instruction.
3. The core Power Policy Unit (PPU) requests that the core transitions from the ON power mode to either the OFF or OFF_EMU power mode.
4. During the L1 or L2 cache clean and invalidate done by the power transition, a RAS error occurs that causes any of the **nCOREFAULTIRQ**, **nCOREERRIRQ**, **nCOMPLEXFAULTIRQ**, or **nCOMPLEXERRIRQ** pins to be asserted.

Implications

The PPU will see the power down request being denied because of the RAS error, however the core will not wake up from the **WFI** instruction and therefore software is not able to handle the error. If the PPU requests the core to power down again, either because it is set to dynamic mode, or because the component programming the PPU requests the power down again, then the second power down might either:

- Complete and power off the core, despite the fact that the error has not been handled.
- Deadlock, preventing the power down from completing.

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

Workaround

The ERXCTLR_EL1.ED bit should be cleared for all the core error records before software sets the CPUPWRCTLR.CORE_PWRDN_EN bit to request a power down. This will cause any error detected during the power down to be ignored. In systems that are particularly concerned about errors during this time, software can clean and invalidate the L1 and L2 caches before clearing the ERXCTLR_EL1.ED bit. This will minimise, but not eliminate, the probability of detecting an error during the powerdown, but at the expense of a longer time to execute the power down sequence.

2012097

TRBE writes to MTE tagged pages might not report external aborts

Status

Fault Type: Programmer Category B

Fault Status: Present in r1p0, r2p0. Fixed in r2p1.

Description

Memory writes due to the Trace Buffer Extension (TRBE) to memory pages that are Tagged via the Memory Tagging Extension and present in the PE caches might fail to report external aborts.

Configurations Affected

This erratum affects all configurations with the BROADCASTMTE pin asserted.

Conditions

1. PE enables the TRBE features.
2. TRBE issues a write to a memory page that is marked MTE Tagged.
3. Interconnect returns a completion response with an error indication - Poison, DErr, or NDErr.

Implications

If the above conditions are met, the PE might fail to record the external abort in TRBSR_EL1.EA (TRBE).

Workaround

If the external abort conditions are non-transient, a read of the TBRE memory buffers will observe the same external abort condition as the write and take a data abort. If the external abort conditions are transient, memory pages used for TBRE can be marked as Untagged.

2017096

Streaming STG and STG2 performance lower than expected with TCF=NONE

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

When writing MTE allocation tags, STG and STG2 instructions might encounter lower than expected performance when SCTLR_ELx.TCF is set to NONE.

Configurations Affected

This erratum affects all configurations.

Conditions

1. PE executes a series of STG or STG2 instruction with SCTLR_ELx.TCF set to NONE.

Implications

If the above conditions are met, the measured bandwidth might be one half of what is expected.

Workaround

Disable store issue prefetching by setting CPUECLTR_EL1[8] to 1. Note that doing so might incur a performance penalty of 0 to 0.3%.

2023111

Utility Bus register accesses to reserved addresses of PE might hang

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

Utility Bus register accesses to some reserved regions of the PE might be ignored and result in a hang.

Configurations Affected

All configurations are affected.

Conditions

This erratum occurs under the following condition:

- Utility Bus Read/Write to a reserved region in PE is executed.

Implications

The Utility Bus register access to DSU might not complete, resulting in a hang.

Workaround

Utility Bus reserved regions of page size in the PE should not be mapped by an MMU onto system memory. Also, these regions should not be made accessible by lower ELs than host.

When using an external debugger, accesses to Utility Bus reserved addresses should be avoided.

2054223

The trace data is not flushed completely during a TSB instruction executed in prohibited region

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

When Embedded Trace Extension (ETE) is in trace prohibited region, and a TSB instruction is executed, any trace data associated with the instructions before the TSB must be observable in memory. Because of this erratum, four bytes of trace data are not pushed to the memory before completing the TSB instruction and those bytes might get lost or might get written to memory in next context.

Configurations Affected

This erratum affects all configurations.

Conditions

1. ETE is enabled.
2. ETE is in trace prohibited region.
3. TRBE is enabled.
4. TSB instruction is executed.

Implications

Four bytes of trace data before TSB instruction might get lost or might get written to memory in next context.

Workaround

To avoid this erratum, software can execute two sequential TSB instructions in any code where one TSB instruction is expected to be required.

2058056

Disabling of data prefetcher with outstanding prefetch TLB miss might cause a deadlock

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0, r2p1. Open.

Description

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

Workaround

- Workaround option 1:
If the following code surrounds the MSR, it will prevent the erratum from happening:
 - `cpp`
 - `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:
 - `ectlr2[14:11], PF_MODE= 4'b1001`

2081180

Executing a WFI or WFE instruction after a STREX instruction might result in a deadlock under specific conditions

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, and r2p0. Fixed in r2p1.

Description

Under certain micro-architectural conditions, executing a WFI or WFE instruction after a STREX that has encountered an external abort might result in a deadlock.

Configurations Affected

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

Conditions

1. Memory tagging is enabled.
2. A STREX instruction executed in MTE precise mode encounters an external abort or poisoned MTE tag.
3. A WFI or WFE instruction is executed.

Implications

If the above conditions are met, then, under specific micro-architectural conditions, the core might deadlock.

Workaround

This erratum can be avoided by inserting a sequence of 16 DMB ST instructions prior to WFI or WFE. Performance impact is expected to be negligible in real systems. This sequence 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,=0xF3A08002
MSR S3_6_c15_c8_2,x0 ; MSR CPUPOR_EL3, X0
LDR x0,=0xFFF0F7FE
MSR S3_6_c15_c8_3,x0 ; MSR CPUPMR_EL3, X0
LDR x0,=0x10002001003FF
MSR S3_6_c15_c8_1,x0 ; MSR CPUPCR_EL3, X0

LDR x0,=0x4
```

```
MSR S3_6_c15_c8_0,x0 ; MSR CPUPSELR_EL3, X0
LDR x0,=0xBF200000
MSR S3_6_c15_c8_2,x0 ; MSR CPUPOR_EL3, X0
LDR x0,=0xFFEF0000
MSR S3_6_c15_c8_3,x0 ; MSR CPUPMR_EL3, X0
LDR x0,=0x10002001003F3
MSR S3_6_c15_c8_1,x0 ; MSR CPUPCR_EL3, X0
```

ISB

2083908

Execution of ST2G instructions in close proximity might cause loss of MTE allocation tag data

Status

Fault Type: Programmer Category B

Fault Status: Present in r2p0. Fixed in r2p1.

Description

Under certain micro-architectural conditions, an ST2G instruction that crosses a 32-byte boundary might not write part of the MTE allocation tag to memory.

Configurations Affected

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

Conditions

1. Memory tagging is enabled.
2. Two or more ST2G instructions are executed in close proximity to the same cache line such that they miss in the L1 cache.
3. One of the ST2G instructions crosses a 32-byte boundary.

Implications

If the above conditions are met, then under specific micro-architectural conditions, the ST2G that crosses the 32-byte boundary might not write part of the MTE allocation tag to memory.

Workaround

This erratum can be avoided by setting CPUACTLR5_EL1[13] to 1. Setting CPUACTLR5_EL1[13] to 1 is expected to result in a small performance degradation for workloads that use MTE (approximately 1.6% when using MTE imprecise mode, 0.9% for MTE precise mode).

2119858

Trace data might get overwritten in TRBE FILL mode

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

Trace Buffer memory size is defined using base pointer and limit pointer in the Trace Buffer Extension (TRBE) programming model. In trace buffer fill mode, TRBE is expected to generate an interrupt and stop the collection of trace after reaching the limit pointer. Due to this erratum, under some microarchitecture conditions, TRBE might roll back to the base pointer after generating an interrupt and continue to write at the base pointer, and up to three cache lines after the base pointer before the collection stops.

Configurations Affected

This erratum affects all configurations.

Conditions

1. ETE and TRBE are enabled.
2. ETE is in a trace allowed region.
3. TRBLIMITR_EL1[2:1] is programmed to 2'b00.

Implications

Due to this erratum, trace data present at the base pointer location and up to three cache lines after the base pointer might get overwritten. The current write pointer also increments by same number of cache line locations.

Workaround

Software can program 256 bytes of ignore packets starting from the base pointer and offset the write pointer TRBPTR_EL1 by 256 bytes before enabling TBE. That ensures oldest trace is not corrupted.

2136059

The CPP instruction will apply to an incorrect EL context

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, and r2p0. Fixed in r2p1.

Description

The **CPP** instruction will not operate on the desired EL as encoded in the instruction.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following condition:

1. A **CPP** instruction is executed.

Implications

The **CPP** instruction will cause the hardware prefetcher to invalidate the hardware prefetcher state associated with an EL other than the EL that is encoded in the instruction.

Workaround

Set CPUACTLR5_EL1[44] which will cause the **CPP** instruction to invalidate the hardware prefetcher state trained from any EL.

2147715

A CFP instruction might not invalidate the correct resources

Status

Fault Type: Programmer Category B
Fault Status: Present in r2p0. Fixed in r2p1.

Description

Executing a CFP instruction under certain conditions might not invalidate resources specified by the instruction.

Configurations Affected

This erratum affects all configurations.

Conditions

1. A CFP instruction is executed.
2. The Exception level specified in the instruction is EL0.
3. $\text{HCR_EL2.TGE}==1$ and $\text{HCR_EL2.E2H}==1$.

Implications

If the previous conditions are met, then the CFP instruction might not invalidate branch predictor resources associated with EL0 context managed by EL2.

Workaround

This erratum can be avoided by setting $\text{CPUACTLR_EL1}[22]=1$. Setting $\text{CPUACTLR_EL1}[22]$ will cause the CFP instruction to invalidate all branch predictor resources regardless of context.

Using this workaround might cause the PE to encounter another erratum. Please refer to erratum ID 2243871 "ELR_ELx[63:48] might hold incorrect value when PE disables address translation" for more details.

2216384

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

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

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 setting CPUACTLR5_EL1[17] to 1 and 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
```

2219376

Enabling TRBE might cause a data write to a page with the wrong ASID when owning Exception level is EL1

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

The Trace Buffer Extension (TRBE) can be used by software to store trace packets from Embedded Trace Extension (ETE) unit to memory. The TRBE unit interfaces with the MMU for translating a virtual address to a physical address. Once a physical address is available, the TRBE unit sends trace packets to the L2 unit to be stored to the memory. The TRBE unit requests a new translation to the MMU when a virtual address crosses the 4K page boundary. Due to this erratum, if a pending translation request from Exception level EL0 or EL1 is serviced after the PE switches context to Exception level EL2, then translation with an incorrect ASID might be provided to the TRBE unit. This can lead to a write to a page with the incorrect ASID.

Configurations Affected

This erratum affects all configurations.

Conditions

1. The TRBE is enabled.
2. Owing Exception level is EL1.
3. TRBLIMITR_EL1.nVM is set to 0, such that the trace buffer pointer addresses are virtual addresses in the EL1&0 translation regime using the current ASID from TTBRx_EL1. This means that the page is marked nG (non-global page).
4. The TRBE unit requests a memory translation request.
5. Before the above memory translation request completes, a context switch occurs from EL0 or EL1, to EL2.

Implications

If the above conditions are met, under certain microarchitectural conditions, incorrect physical address and page attributes from a different ASID might be provided to the TRBE unit. The TRBE might then write to memory using incorrect page attributes from another ASID, leading to a write that is not expected.

Workaround

The software should use global pages ($nG=0$) for the pages that are used by the TRBE to store data when owning Exception level is EL1.

2224489

TRBE might cause a data write to an out-of-range address which is not reserved for TRBE

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

Trace buffer memory size is defined using base pointer and limit pointer in Trace Buffer Extension (TRBE) programming model. TRBE is expected to wrap to base pointer without crossing the limit pointer. Because of this erratum, under some conditions, TRBE might generate a write to the next virtually addressed page following the last page of TRBE address space.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Embedded Trace Extension (ETE) and TRBE are enabled.
2. ETE is in trace allowed region.
3. TRBE current pointer is at last page of Trace buffer.
4. TRBE requests translation for the last page.
5. LS indicates to TRBE that it is unable to service the translation request.

Implications

When previous conditions are met under rare microarchitectural conditions, TRBE might incorrectly generate a data write to the next virtually addressed page following the last page of Trace Buffer. This can lead to data corruption if that page is currently used by another application and result in loss of trace up to 64 bytes.

Workaround

The software can mark as not valid the next page following the last TRBE page, meaning the errant access will generate a Translation Fault buffer management event. This will prevent the data corruption but will not prevent the loss of trace data.

2267065

A CFP instruction might execute with incorrect upper ASID or VMID bits

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

The upper 8 bits of ASID or VMID might be incorrect for a CFP instruction.

Configurations Affected

This erratum affects all configurations.

Conditions

1. A CFP is executed with ELO target execution context and {HCR_EL2.TGE, HCR_EL2.E2H} is {1,1} and TCR_EL2.AS=0.
2. A CFP is executed at EL2 or EL3 and the target execution context is ELO or EL1 and VTCR_EL2.VS=0.

Implications

If either of the previous conditions are met, then the CFP instruction might not invalidate branch predictor resources associated with ELO or EL1 contexts.

Workaround

This erratum can be avoided by setting CPUACTLR_EL1[22]=1. Setting CPUACTLR_EL1[22] will cause the CFP instruction to invalidate all branch predictor resources regardless of context.

2282622

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, r1p0, r2p0, r2p1. Open.

Description

A *Processing Element* (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

This erratum occurs under the following 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/PFRM 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.

2291219

Denied power down request might prevent completion of future power down request

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, and r2p0. Fixed in r2p1.

Description

If a Processing Element (PE) initiates a power down request that is ultimately denied due to an external event, a future power down request might fail to complete.

Configurations Affected

This erratum affects all configurations.

Conditions

1. PE initiates a power down request (ON to OFF state transition) by setting CORE_PWRDN_EN and executing a WFI instruction.
2. PE completes the hardware flush of its caches.
3. An event, such as an external interrupt, causes an abort of the power down request.
4. PE returns to the ON state without performing a hardware reset.

Implications

If the above conditions are met, the PE might fail complete a subsequent power down request resulting in a deadlock.

Workaround

This erratum can be avoided by setting CPUACTLR2_EL1[36] to 1 before the power-down sequence that includes setting the CORE_PWRDN_EN bit, and executing a WFI. This bit should be cleared on exiting WFI by any mechanism other than reset.

2371105

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

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, and r2p0. Fixed in r2p1.

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.

2381390

A continuous stream of incoming DVM syncs may cause TRBE to prevent the core from forward progressing

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

A continuous stream of incoming *Distributed Virtual Memory* (DVM) syncs might cause the *Trace Buffer Extension* (TRBE) to prevent the core from forward progressing, while executing a WFX.

Configurations Affected

This erratum affects all configurations.

Conditions

The erratum occurs if all the following conditions are met:

- The *Processing Element* (PE) executes a WFE or WFI instruction.
- TRBE is in use and needs to write trace data to its buffer.
- A continuous stream of DVM sync operations is received from other PEs.

Implications

When all of the above conditions are met, the PE might be prevented from entering WFE or WFI, and the pending WFE or WFI operation cannot be interrupted.

Workaround

There is no workaround.

2701952

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, r1p0, r2p0, r2p1. 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.

2742423

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, r1p0, r2p0, and r2p1. 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.

2768515

The core might deadlock during powerdown sequence

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0, and r2p1. 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 power-down sequence as described in 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.

2778471

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, r1p0, r2p0, r2p1. 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.

3003018

PE executing DRPS during Debug Halt under Double Fault condition will not execute properly

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0 and r2p1. Open

Description

When a DRPS instruction is executed in Debug Halt state, a double fault should cause implicit ESB according to the *Arm Architecture Reference Manual for A-profile architecture* when (SCR_EL3.EA == '1' && SCR_EL3.NMEA == '1' && PSTATE.EL == **EL3**). However, the *Processing Element* (PE) will only execute part of the instruction for this case.

Configurations affected

This erratum affects all configurations with double fault extension.

Conditions

This erratum occurs under the following conditions:

1. The PE is in Debug Halt state.
2. Software is currently executing at EL3 Exception level.
3. SCTLR_EL3.IESB == '0'
4. SCR_EL3.EA == '1' && SCR_EL3.NMEA == '1' indicating double fault.

Implications

The DRPS instruction is not executed correctly.

Workaround

When executing a DRPS instruction in EL3, set SCTLR_EL3.IESB to override double fault. Doing this will force the correct DRPS execution sequence to occur.

3038569

TRBE 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, r1p0 and r2p0. Fixed in r2p1.

Description

The *Trace Buffer Extension* (TRBE) uses the Stage-1 translation regime of the owning exception level in the owning Security state. Due to this erratum, the TRBE 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 TRBE.

Conditions

This erratum occurs under the following conditions:

1. TRBE is enabled.
2. TBBPTR_EL1 and TBLIMITR_EL1 are configured to include a virtual address VA_X.
3. TBLIMITR_EL1.nVM is 0.
4. A valid Stage-1 translation exists for the virtual address VA_X.
5. If Stage-2 is enabled, a valid Stage-2 translation exists for the intermediate physical address IPA_X for the virtual address VA_X.
6. 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.
7. 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 TRBE might write to VA_X rather than generating a fault. This might allow malicious software with control over TRBE 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 TRBE unless the hypervisor can handle writes to any pages mapped at Stage-2.

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

3099212

PE might execute instructions consistent with previous context-synchronized state when SCR_EL3.EEL2 is changed

Status

Fault Type: Programmer Category B

Fault Status: Present in r0p0, r1p0, r2p0, and r2p1. Open.

Description

When SCR_EL3.EEL2 is modified to a different value and a context synchronization event occurs, the PE might execute instructions consistent with previous context-synchronized state of SCR_EL3.EEL2.

Configurations affected

This erratum affects all configurations.

Conditions

1. The field SCR_EL3.EEL2 is changed to a different value than last context-synchronized value.
2. A context synchronization event occurs.
3. Execution of any instruction with a behavior that depends on the value of SCR_EL3.EEL2.

Implications

If the previous conditions are met, instructions might use control information saved consistent with the previous context, and might result in unexpected exceptions and load/store alignment sizes.

Workaround

This issue can be worked around by changing the value of any of these fields in SCR_EL3 at the same time as changing the value of the field EEL2:

1. SCR_EL3.EA
2. SCR_EL3.API
3. SCR_EL3.NMEA

Alternatively, execute the following code sequence after changing SCR_EL3.EEL2, and prior to returning to a lower EL:

```
// Toggle the value of SCR_EL3.EA, context synchronize, then restore the value of SCR_EL3.EA
MRS x0,SCR_EL3
```

```
LDR x1,=0x8  
EOR x2,x0,x1  
MSR SCR_EL3,x2  
ISB  
MSR SCR_EL3,x0
```

Category B (rare)

2982956

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, r1p0, r2p0, and r2p1. 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 Watchpoint 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 `VTCTR_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

1786338

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 r1p0.

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_ELO 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_ELO 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.

1787272

TSB instruction completion can be delayed when executed in region where trace is allowed

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0. Fixed in r1p0.

Description

If the Embedded Trace Macro Extension (ETE) unit is enabled and a TSB instruction is executed, then trace packets generated due to instructions executed before the TSB instruction must be output from the ETE unit. If the Trace Buffer Extension (TRBE) unit is also enabled, then these trace packets must be output from the TRBE unit before the TSB instruction can complete. Due to this erratum, under some conditions the TSB instruction completion might take an additional 8192 core clock cycles than normal.

Configurations affected

This erratum affects all configurations.

Conditions

1. The ETE unit is enabled.
2. Tracing is currently allowed in the ETE unit.
3. The TRBE unit is enabled.
4. A TSB instruction is executed.
5. The ETE unit has less than 4 bytes left to be output.
6. The ETE unit is not generating new trace packets.

Implications

If the above conditions are met, the TSB instruction might take an additional 8192 core clock cycles to complete.

Workaround

Software should execute the TSB instruction in a prohibited region. There is no workaround if the TSB instruction is executed in a trace allowed region.

1799975

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

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0. Fixed in r1p0.

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 Data Cache Zero by VA (DC ZVA) falls in the upper portion of the cache line that the watchpoint does not target, the Fault Address Register (FAR) (or External Debug Watchpoint Address Register (EDWAR) if setup for Debug Halt) 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.

EDWAR contains target address of DC ZVA if enabled for Debug Halt.

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.

1804175

CTI event from the core to the external DebugBlock might be dropped

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r1p0.

Description

The PE generates input trigger events which are routed to Cross-Trigger Interface (CTI) via the external DebugBlock. 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 the completion of the processing of the previous CTI event.

Implications

The earlier CTI event might be dropped.

Workaround

This erratum has no workaround.

1804563

Trace Buffer Extension unit might write trace packets to memory using incorrect memory page attributes

Status

Fault Type: Programmer Category C

Fault status: Present in r0p0. Fixed in r1p0.

Description

Trace Buffer Extension (TRBE) can be used by software to store trace packets from Embedded Trace Extension (ETE) unit to memory. The TRBE unit interfaces with the MMU for translating a virtual address to a physical address. Once a physical address is available the TRBE unit sends trace packets to the L2 unit to be stored to memory. The TRBE unit requests a new translation to the MMU when a virtual address crosses the 4K page boundary. Due to this erratum, if this new translation request is completed while the TRBE unit is sending trace packets to L2 from a previous translation request, then the trace packets might incorrectly use cache and shareability attributes, Page Based Hardware Attributes (PBHA), and Non-Secure attributes (NS) from the new translation request.

Configurations affected

This erratum affects all configurations.

Conditions

1. The TRBE unit is enabled.
2. The TRBE unit is sending trace packets to the L2 unit using the last 64-byte address range of a 4K memory page.
3. The TRBE unit initiates a new memory translation request for the first 64-byte address range of the next 4K memory page.
4. The response for the new memory translation request completes before pending trace packets are accepted by the L2 unit.
5. Memory page attributes are different between these two 4K memory pages.

Implications

If the above conditions are met, the TRBE unit might write trace packets to memory with incorrect cache, shareability attributes, PBHA and NS from the new translation request related to next 4K page.

Workaround

Software should use consistent page attributes for all pages within the buffer.

1817593

Persistent faults on speculative elements of SVE First-fault gather-load instructions might result in deadlock

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0. Fixed in r1p0.

Description

Double-bit ECC errors or bus faults on a non-first active element of an SVE First-fault gather load might result in deadlock.

Configurations affected

This erratum affects all configurations.

Conditions

1. A double-bit ECC error or bus fault occurs on a non-first active element of an SVE First-fault gather-load instruction.
2. The double-bit ECC error or bus fault must be persistent, meaning on repeated attempted executions of the instruction, the fault consistently re-occurs.
3. Certain internal timing conditions concerning the execution order of the non-first active element relative to the first active element exist.

Implications

If the above conditions are met, the core can deadlock. An interrupt can be recognized, but the SVE First-faulting gather-load instruction makes no forward progress in the presence of persistent ECC double-bit errors or bus faults that occur on elements other than the first active element.

Workaround

No workaround is expected to be required. RAS error handling and recovery techniques cover this scenario.

1827136

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

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0. Fixed in r1p0.

Description

In Debug state with SCTL_R_EL_x.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. SCTL_R_EL_x.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 SCTL_R_EL_x.IESB before performing memory uploads or downloads in Debug state using memory access mode.

1838906

Noncompliance with prioritization of Exception Catch debug events

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0, r2p1. 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.

1851171

Transient L2 tag double bit Errors might cause data corruption

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r1p0.

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

This erratum affects all configurations.

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.

1851323

Incorrect trace timestamp value when self-hosted trace is disabled

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r1p0.

Description

If the Embedded Trace Extension (ETE) unit is enabled and configured with global timestamp tracing enabled, the timestamp value might be incorrectly sourced.

Configurations Affected

This erratum affects all configurations.

Conditions

The trace timestamp might be incorrect when:

1. The ETE unit is enabled.
2. The ETE unit is configured with global timestamp tracing enabled.
3. Tracing is allowed.
4. Self-hosted trace is disabled.
5. Timestamp control is programmed to use a virtual counter value.

Implications

The trace timestamp might have an incorrect value from a virtual counter instead of being sourced from CoreSight time.

Workaround

The external debugger can program either:

- TRFCR_EL2.TS == 0b11, or
- TRFCR_EL2.TS == 0b00 and TRFCR_EL1.TS == 0b11.

Software should preserve the values written by the debugger.

1851816

The MPAM value associated with MMU descriptor fetch requests might be incorrect

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

Description

The MPAM value associated with MMU descriptor fetch requests could be incorrect when performing address translation on behalf of *Address Translation* (AT) instructions or the table walk prefetcher.

Configurations Affected

This erratum affects all configurations.

Conditions

1. An MMU descriptor fetch request is made on behalf of AT instructions or the table walk prefetcher.

Implications

If the above condition is met, the core generates a memory-system request for the translation table walk using the MPAM ID for the:

1. Context associated with an AT instruction instead of the context that executed the instruction.
2. ELO context for translations generated by the table walk prefetcher trained in EL1 or EL2 context when $\text{HCR_EL2}\{E2H, TGE\} == \{1, 1\}$.

Workaround

There is no workaround.

1855551

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 r1p0.

Description

Under certain conditions, the `ERRORMISCO_EL1.SUBARRAY`, `ERROSTATUS.CE`, and `ERROSTATUS.DE` values recorded for ECC errors in the L1 data cache might be incorrect.

Configurations Affected

This erratum affects all configurations.

Conditions

1. The L1 data cache contains both a single-bit and a 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 `ERRORMISCO_EL1.SUBARRAY`, `ERROSTATUS.CE`, and `ERROSTATUS.DE` might have an incorrect values.

Workaround

There is no workaround for this erratum.

1859562

Incorrect read value for the Trace ID Register 3 SYSSTALL field

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r1p0.

Description

The Trace ID Register 3 (TRCIDR3) in the trace registers contains an incorrect value in the SYSSTALL field.

Configurations Affected

All configurations are affected.

Conditions

Software reads the TRCIDR3 register.

Implications

The TRCIDR3.SYSSTALL field contains the incorrect value of 0x1, indicating that PE stalling is permitted, instead of containing the expected value of 0x0 as stalling of the PE is not implemented. Any software using this field to check if stalling of the PE is permitted might not correctly identify it.

Workaround

Software should ignore the value of this field.

1862651

Incorrect read value for External Debug Processor Feature Register

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r1p0.

Description

Under certain conditions, External Debug Processor Feature Register (EDPFR) returns an incorrect read value for the GIC field.

Configurations Affected

All configurations are affected.

Conditions

1. GICCDISABLE input pin is set.
2. Debugger reads the EDPFR register.

Implications

The EDPFR.GIC field incorrectly reports the value 0x3 indicating that System register interface to version 4.1 of the GIC CPU interface is supported, instead of the expected value of 0x0, as GIC CPU interface system registers is not implemented when GIC CPU interface is disabled.

Workaround

There is no workaround.

1865453

The values for fields ID_AA64ZFR0_EL1.{SM4,SHA3,AES} read incorrectly as non-zero

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r1p0.

Description

If configured without Cryptographic Extension support, the PE will incorrectly report non-zero values for certain SVE feature identification registers.

Configurations Affected

This erratum affects all configurations.

Conditions

1. The PE is configured with no Cryptographic Extension support.
2. A MRS from ID_AA64ZFR0_EL1 is executed.

OR

1. The PE is configured with Cryptographic Extension support and the CRYPTODISABLE pin is set.
2. A MRS from ID_AA64ZFR0_EL1 is executed.

Implications

If the above conditions are met, the values for fields ID_AA64ZFR0_EL1.{SM4,SHA3,AES} will incorrectly read as non-zero.

Workaround

There is no workaround.

1868638

The core does not treat the BAS field of the Debug Breakpoint Control Register as RES1

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0. Fixed in r1p0.

Description

The core is not treating the BAS field of the Debug Breakpoint Control Register (DBGBCR) as RES1, as specified in the Arm Architecture Reference Manual. When AArch32 is not supported at any Exception level, then the DBGBCR<n>.BAS field bits are RES1. This field should be written to 0b1111 by software and ignored by hardware.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Hardware breakpoint is enabled in address match mode.
2. The DBGBCRn_EL1.BAS field is programmed to any value other than 0b1111.

Implications

If the above conditions are met, a breakpoint exception might not be taken as required by the Arm Architecture.

Workaround

This erratum can be avoided if software properly writes 0b1111 to the RES1 bits for the DBGBCR<n>.BAS field.

1870363

L2 data RAM may fail to report corrected ECC errors

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r1p0.

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.

1875555

Compare and Swap (CAS) instructions with stack pointer as base register are incorrectly treated as checked accesses

Status

Fault Type: Programmer Category C

Fault Status: Present in r1p0. Fixed in r2p0.

Description

Compare and Swap(CAS) instructions with stack pointer as base register and no offset are incorrectly treated as checked accesses when MTE tag checking is enabled.

Configurations affected

This erratum affects all configurations.

Conditions

1. MTE tag checking is enabled.
2. CAS (any flavor) with stack pointer as base register is executed.

Implications

The CAS instruction under consideration will be treated as a "checked" access, triggering unexpected tag check faults. Typical bring-up software is not expected to run into this scenario on test silicon.

Workaround

There is no workaround.

1875745

A Checked load that fails a Tag Check could set the ESR to an incorrect value

Status

Fault Type: Programmer Category C
Fault Status: Present in r1p0. Fixed in r2p0.

Description

Under certain conditions, memory access by a Checked load that generates a Tag Check fail on some bytes and an external data abort on other bytes could result in the setting of an incorrect value in the Exception Syndrome Register (ESR).

Configurations Affected

This erratum affects all configurations.

Conditions

1. Memory tagging is enabled and a Checked load that crosses a 16B aligned boundary performs memory access.
2. The first half of the access sees an ECC error or generates an external data abort.
3. The second half of the access generates a Tag Check fail.

Implications

If the above conditions are met, the ESR_ELx.FnV and ESR_ELx.EC values could be incorrect. ESR_ELx.FnV could be set when the FAR contents are incorrect. ESR_ELx.EC could be incorrectly set to 6'b010001. It is expected that software can handle this scenario on test silicon used for software bringup.

Workaround

There is no workaround.

1884880

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

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0, r2p1. 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 the 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.

1893664

Accessing a memory location using mismatched shareability attributes when MTE tag checking is enabled might lose coherency or deadlock

Status

Fault Type: Programmer Category C

Fault Status: Present in r1p0. Fixed in r2p0.

Description

A PE accessing a same physical memory location with mismatched shareability attributes and requiring a read of Memory Tagging Extension (MTE) tags might lose coherency or deadlock.

Configurations Affected

This erratum affects all configurations.

Conditions:

1. PE accesses a physical memory location using cacheable and non-shareable attributes.
2. PE performs a clean and invalidate to satisfy requirements for shareability aliasing.
3. PE performs an untagged store to the same physical memory location using cacheable and shareable attributes.
4. PE performs a tagged memory access to the same physical address.

Implications

If the above conditions are met, the PE might lose the store data from condition 3 or fail to make forward progress on a load to the same physical address.

Workaround

Avoid using mismatched shareability attributes for aliases of the same memory location for tagged pages.

1896171

Access to External Debug Auxiliary Processor Feature Register might incorrectly return an error response

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

Description

An External Debug access to External Debug Auxiliary Processor Feature Register (EDAA32PFR) incorrectly gets an error response when OSLock is set.

Configurations Affected

This erratum affects all configurations.

Conditions

1. OSLSR_EL1.OSLK bit is set.
2. A memory mapped access is made to the EDAA32PFR register.

Implications

The access would incorrectly get an error response when no error was expected due to OSLock.

Workaround

Debugger should clear OSLock before accessing the register.

1899211

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

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

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.

1899435

PFG duplicate reported faults through a Warm reset

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

Description

Under 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. ERROPFGCDN is set with a non-zero countdown value.
2. ERROPFGCTL is set to generate a pseudo-fault with ERROPFGCTL.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 ERROPFGCTL control bits before asserting a Warm reset.

1909702

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

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0, r2p1. 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.

1911676

TFSR contents might be incorrect after executing a page crossing SVE predicated load instruction

Status

Fault Type: Programmer Category C

Fault Status: Present in r1p0, r2p0. Fixed in r2p1.

Description

Under certain conditions, TSFR_ELx bit[0] might be incorrect when an SVE predicated instruction accesses bytes that cross the 0xFFFF_FFFF_FFFF_FFFF boundary.

Configurations Affected

This erratum affects all configurations.

Conditions

1. SVE predicate load is executed at EL1 or EL2 with HCR_EL2.E2H=1 and accesses bytes crossing the 0xFFFF_FFFF_FFFF_FFFF boundary.
2. Imprecise Checked access is generated for bytes in the first page and fails Tag Check.
3. Second page has no active elements.

Implications

If the above conditions are met, TFSR_ELx bit[0] might be incorrectly updated instead of TFSR_ELx bit[1].

Workaround

This erratum has no workaround.

1919240

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

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

Description

If Pseudofault Injection is enabled for the PE node (ERR1PFGCTL.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 (ERR1PFGCTL.CDNEN=0x1), then the PE might deadlock.

Configurations Affected

This erratum affects all configurations.

Conditions

1. ERR1PFGCTL.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. ERR1PFGCTL.CDNEN is set to 0x1 to enable Pseudofault Injection.

Implications

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

Workaround

Ensure ERR1PFGCTL.CDNEN=0x0 before entering Debug State and while executing in Debug State.

1920415

Trace Buffer might write trace packets to memory using incorrect cache attributes

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

Description

Due to this erratum, a translation request from the Trace Buffer Extension (TRBE) unit might incorrectly use the write-back Cacheability attribute when both TRBLIMITR_EL1.nVM and HCR_EL2.CD are set.

Configurations Affected

This erratum affects all configurations.

Conditions

1. The TRBE is enabled.
2. TRBLIMITR_EL1.nVM is set.
3. HCR_EL2.CD is set.
4. Stage 2 translation is enabled.
5. The TBRE unit requests a translation.

Implications

If the above conditions are met, TRBE translations would be incorrectly marked as write-back cacheable instead of being assigned the correct non-cacheable attribute. As a result, TRBE could write trace packets to memory using the incorrect Cacheability attributes.

Workaround

There is no workaround.

1920634

A Checked store with poisoned tags might result in a Tag Check Fail instead of taking an SError interrupt exception

Status

Fault Type: Programmer Category C

Fault Status: Present in r1p0. Fixed in r2p0.

Description

Under certain conditions, poisoned data that is flagged when the Allocation Tag is accessed from memory by a Checked store that is executing in MTE imprecise mode, might result in a Tag Check Fail instead of reporting an SError interrupt exception.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Memory tagging is enabled.
2. A Checked store that is executing in imprecise mode performs a memory access.
3. The Allocation Tag is returned with the poison indication.

Implications

If the above conditions are met, then the Checked store might result in a Tag Check Fail being asynchronously accumulated instead of reporting an SError interrupt exception.

Workaround

There is no workaround.

1920871

MPAM value associated with translation table walk request might be incorrect

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

Under some scenarios, MPAM value associated with translation table walk request might be incorrect when context changes along with security state.

Configurations Affected

All configurations are affected.

Conditions

1. Translation table walk request attempted before a context switch but is not completed until after a context change where the secure state changes.

Implications

MPAM value associated with the table walk request might be incorrect.

Workaround

There is no workaround.

1925506

Unsupported atomic fault due to memory type defined in first stage of translation might result in exception being taken to EL2

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

Description

Under certain conditions, when far atomics are not supported by the system, an unsupported atomic fault due to the memory type defined in the first stage of translation might result in an exception being taken to EL2.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Device memory type is defined in the first stage of translation for the atomic instruction.
2. HCR_EL2.VM, HCR_EL2.FWB, and HCR_EL2.CD bits are set.
3. The system does not support far atomics.

Implications

If the above conditions are met, an exception is incorrectly taken to EL2.

Workaround

There is no workaround.

1926908

Access with additional latency from alignment (LDST_ALIGN_LAT) PMU event does not count

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

Description

The LDST_ALIGN_LAT, Access with additional latency from alignment, PMU event will not count correctly.

Configurations Affected

This erratum affects all configurations.

Conditions

1. One of the PMU event counters is configured to count the 0x4020, LDST_ALIGN_LAT PMU event.

Implications

The LDST_ALIGN_LAT PMU event will not be counted. The counter value for the event will not be correct and therefore cannot be used.

Workaround

There is no workaround.

1927566

ERR0MISCO_EL1.SUBARRAY value for ECC errors in the L1 data cache might be incorrect

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

Description

Under certain conditions, the ERR0MISCO_EL1.SUBARRAY value recorded for ECC errors in the L1 data cache might be incorrect.

Configurations Affected

This erratum affects all configurations.

Conditions

1. A load, store, or atomic instruction accesses multiple banks of the L1 data cache.
2. One of the banks accessed has an ECC error.

Implications

If the above conditions are met, then ERR0MISCO_EL1.SUBARRAY might have an incorrect value. The remaining fields of the ERR0MISCO_EL1 register remain correct.

Workaround

There is no workaround.

1929989

Event Stream from the Virtual Counter is not correctly disabled by VHE in Secure State

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0. Fixed in r2p0.

Description

While the PE is executing in Secure State with Secure EL2 enabled (SCR_EL3.EEL2=0x1), the Event Stream generated from the Virtual Counter is not correctly disabled when HCR_EL2.(E2H, TGE)=(0x1, 0x1).

Configurations Affected

This erratum affects all configurations.

Conditions

1. The PE is executing in Secure State and Secure EL2 is enabled (SCR_EL3.EEL2=0x1).
2. CNTKCTL_EL1 is configured to generate an Event Stream from the Virtual Counter.
3. HCR_EL2.(E2H, TGE)=(0x1, 0x1) is configured to disable generation of an Event Stream from the Virtual Counter.

Implications

The Event Stream will be generated incorrectly.

Workaround

Secure EL2 can disable the generation of the Event Stream from the Virtual Counter by writing CNTKCTL_EL1.

1938354

Incorrect fault status code might be reported in Trace Buffer Extension register TRBSR_EL1.FSC

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

The Trace Buffer Extension (TRBE) unit can be used by software to store trace packets from the Embedded Trace Extension (ETE) unit to memory. Due to this erratum, a translation request initiated by the TRBE which encounters multiple hits in the TLB might report an incorrect fault status code in TRBSR_EL1.FSC.

Configurations Affected

This erratum affects all configurations.

Conditions

1. ETE is enabled.
2. ETE is in trace allowed region.
3. TRBE is enabled.
4. TRBE requests a memory translation.
5. 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 one of the following behaviors might be observed.

1. The fault status code reported in TRBSR_EL1.FSC might incorrectly indicate an illegal fault status code or
2. The fault status code reported in TRBSR_EL1.FSC might incorrectly indicate another code instead of the correct TLB Conflict fault code or
3. A fault might be incorrectly reported when not expected with fault status code in TRBSR_EL1.FSC indicating TLB conflict fault.

Workaround

There is no workaround.

1949697

A Checked store that crosses a page boundary might not perform a Tag Check

Status

Fault Type: Programmer Category C

Fault Status: Present in r1p0, r2p0. Fixed in r2p1.

Description

Under certain micro-architectural conditions, a page-crossing Checked store executing in MTE imprecise mode might not perform a Tag Check if the second half of the memory access is Unchecked.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Memory tagging is enabled.
2. A page-crossing Checked store performs memory access where the first half is an Imprecise Checked access and the second half is an Unchecked access.

Implications

If the above conditions are met under specific micro-architectural conditions, Tag Check might not be performed for the first half of the memory access.

Workaround

This erratum has no workaround.

1971496

VMID value in trace packets might be incorrect

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

CX bit in Trace Filter Control Register EL2 (TRFCR_EL2) enables VMID trace. This bit is ignored under some conditions and VMID field in trace elements might be zero.

Configurations affected

This erratum affects all configurations.

Conditions

The erratum occurs under the following conditions:

1. The Embedded Trace Extension unit is enabled.
2. Self hosted trace is enabled.
3. CID_EL2 and VMID trace are allowed (TRCCONFIGR.VMID == 1 AND TRFCR_EL2.CX == 1)
4. Core is executing in Secure EL0/EL1 with Secure EL2 disabled (SCR_EL3.NS == 0 AND SCR_EL3.EEL2 == 0)

Implications

If above conditions are met, then VMID field in trace elements might be zero, potentially leading to the generation of incorrect context elements by the trace unit.

Workaround

No workaround is required as the architecture is expecting that EL3 will clear TRFCR_EL2 as part of a state switch in these conditions.

1975917

AMU Event 0x0011, Core frequency cycles might increment incorrectly when the core is in WFI or WFE state

Status

Fault Type: Programmer Category C.

Fault Status: Present in r0p0, r1p0, r2p0, r2p1. Open.

Description

The core frequency cycles Activity Monitor Unit (AMU) event may not count correctly when the core is in *Wait For Interrupt* (WFI) or *Wait For Event* (WFE) state and the clocks in the core are enabled.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. The architected activity monitor counter register 0 (AMEVCNTR00) is enabled.
2. The core executes WFE instructions in any version or the core executes WFI instructions in versions prior to r2p1.
3. The clocks in the core are never disabled, or
4. The clocks in the core are temporarily enabled without causing the core to exit WFE state in any version or WFI state in versions prior to r2p1 due to one of the following events:
 - A system snoop request that must be serviced by the core L1 data cache or the L2 cache.
 - A cache or *Translation Lookaside Buffer* (TLB) maintenance operation that must be serviced by the core L1 instruction cache, L1 data cache, L2 cache, or TLB.
 - An access on the Utility bus interface.
 - A *Generic Interrupt Controller* (GIC) CPU access or debug access through the *Advanced Peripheral Bus* (APB) interface.

Implications

The core frequency cycles AMU event will continue to increment when clocks are enabled even though the core is in WFE state for any version or WFI state for versions prior to r2p1. Arm expects this to be a minor issue as the resulting discrepancies will likely be negligible from the point of view of consuming these counts in the system firmware at the 1ms level.

The WFI condition was fixed in version r2p1, but the issue was not fully resolved for WFE. Therefore, the WFE condition exists on all versions, whereas the WFI condition is only present in r0p0, r1p0, and r2p0 versions.

Workaround

There is no workaround.

1980906

Reset Catch debug event might not cause core to enter Debug state immediately after Cold reset

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

The core might not enter Debug state immediately after Cold reset is deasserted when Reset Catch debug event is enabled and halting is allowed.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Reset Catch debug event is enabled.
2. Halting is allowed.
3. Cold reset is deasserted.

Implications

If the conditions are met, then the core might not enter Debug state after Cold reset is deasserted and before the first instruction is executed. The core will enter Debug state either before executing any instruction or after executing few instructions.

Workaround

There is no workaround.

1986267

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, r1p0, r2p0. Fixed in r2p1.

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.

1989365

Floating-point Operations speculatively executed PMU events are not counted

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

The following PMU events do not count correctly:

- 0x8014, FP_HP_SPEC, Half-precision floating-point Operations speculatively executed
- 0x8018, FP_SP_SPEC, Single-precision floating-point Operations speculatively executed
- 0x801C, FP_DP_SPEC, Double-precision floating-point Operations speculatively executed

Configurations Affected

This erratum affects all configurations.

Conditions

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

- 0x8014, FP_HP_SPEC
- 0x8018, FP_SP_SPEC
- 0x801C, FP_DP_SPEC

Implications

PMU event counters configured for these PMU events do not count.

Workaround

There is no workaround.

2000010

Execution of STG instructions in close proximity might incorrectly write MTE Allocation Tag to memory more than once

Status

Fault Type: Programmer Category C

Fault Status: Present in r2p0. Fixed in r2p1.

Description

Under certain micro-architectural conditions, an STG instruction might write MTE Allocation Tag to memory more than once.

Configurations Affected

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

Conditions

1. Memory tagging is enabled.
2. Two or more STG instructions that write both Allocation Tag and Data are executed in close proximity.
3. Above STG instructions access the same cache line address but different 32 bytes in memory.

Implications

If the above conditions are met, then under specific micro-architectural conditions Allocation Tag for the entire cache line may be written to memory twice. This is not expected to be an issue as Allocation Tags are written by only one software agent at a time. The value of Allocation Tag will not change between these two writes since there will not be another write to Allocation Tag from another PE.

Workaround

There is no workaround.

2002779

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, r1p0, r2p0. Fixed in r2p1.

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

This 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.

2017087

DSB might not guarantee completion of direct reads of L2 cache memories

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

Direct reads of internal memories are implemented using a SYS #6, C15, C0, #0, <Xt> instruction executed in EL3. In response to this instruction, the PE reads an internal memory and places the contents in implementation defined DDATAx registers. A DSB is intended to guarantee completion of the memory access. If the targeted RAMs are the L2 tag, L2 victim, or L2 data RAM, a DSB might not provide this guarantee.

Configurations Affected

This erratum affects all configurations.

Conditions

1. PE executes a SYS #6, C15, C0, #0, <Xt> instruction, where Xt specifies the L2 tag, L2 data, or L2 victim RAMs.
2. PE executes a DSB.
3. PE reads the DDATAx registers.

Implications

If the above conditions are met, along with specific microarchitectural conditions, the DDATAx registers may not be updated when the DSB completes.

Workaround

When performing direct memory accesses to L2 cache memories do the following:

1. Set CPUACTLR2_EL1[46].
2. Perform the direct memory accesses.
3. Clear CPUACTLR2_EL1[46].

Note that setting CPUACTLR2_EL1[46] incurs a 1-2% performance penalty. Thus, CPUACTLR2_EL1[46] should not be set by default.

2018317

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, r1p0, r2p0. Fixed in r2p1.

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

The following debug component shares the offset alias with the EDITR register when the PE is configured with 20-PMUs:

- PMU - PMEVCNTR16[63:32] - Event Counter 16

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.

2025108

Corrupted register state results from executing specific form of SEL instruction followed by SVE AESMC or AESIMC instruction

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

Under certain conditions, execution of two SVE instructions, either SEL(vectors) followed by AESMC or SEL(vectors) followed by AESIMC, might result in corruption of a destination vector register.

Configurations affected

This erratum affects configurations with CRYPTO==TRUE.

Conditions

The following SVE instruction sequence is required

1. PE executes SEL <Zd>.B, <Pg>, <Zn>.B, <Zm>.B
2. PE executes either AESMC <Zd>.B, <Zd>.B or AESIMC <Zd>.B, <Zd>.B

Implications

The sequence of instructions described in the conditions above are not expected to occur in real code, because they do not perform useful computation. As such, no impact is expected to real systems.

Workaround

Because the code sequences for this erratum are not expected to occur in real code, no workaround is required.

2050953

External aborts for streaming writes to MTE tagged pages may report multiple errors

Status

Fault Type: Programmer Category C

Fault Status: Present in r1p0, r2p0. Fixed in r2p1.

Description

If a streaming write to a memory page with Memory Tagging Extension (MTE) tagging enabled receives an External abort, it may report multiple SError aborts.

Configurations Affected

This erratum affects all configurations with the BROADCASTMTE pin asserted.

Conditions

1. The Processing Element (PE) generates a write of a full cache line to a memory page that is marked MTE Tagged.
2. A transaction issued on the CHI interconnect on behalf of the streaming write receives an External abort from the interconnect

Implications

If the above conditions are met, the PE might report multiple SError aborts. External aborts received from the interconnect represent error conditions in the system, such as accesses to unmapped devices and uncorrectable ECC errors. These conditions are more severe than the possibility of the PE reporting multiple SError aborts.

Workaround

There is no workaround.

2052424

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, r1p0, r2p0. Fixed in r2p1.

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. DBG BXVR<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.

2054222

Trace data lost during collection stop in TRBE

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

When a collection stop event occurs in the Trace Buffer Extension (TRBE), trace collection from the Embedded Trace Extension (ETE) is stopped and the data in the TRBE buffers are flushed to memory. When this occurs under certain micro-architectural timing conditions, 64 bytes of trace data might get lost and replaced with Ignore bytes. This does not result in a current pointer mismatch.

Configurations affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. ETE and TRBE are enabled.
2. ETE is in a trace-allowed region.
3. A collection stop event occurs in TRBE.

Implications

When the above conditions are met, 64 bytes of trace data might get lost and replaced with Ignore bytes while getting written to memory.

Workaround

The erratum has no workaround.

2058367

L3D_CACHE_ALLOC PMU inaccurate when using WriteEvictOrEvict transactions

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

When the L2 cache issues a WriteEvictOrEvict transaction for a L2 copyback, the L3D_CACHE_ALLOC PMU event is not counted, even though it might cause an L3 cache allocation.

Configurations Affected

This erratum affects all configurations that enable WriteEvictOrEvict transactions through CPUECLTR_EL1[45]=1.

Conditions

1. CPUECLTR_EL1[45] is set to 1 (default value).
2. PE is configured to count PMU event 0x29 L3D_CACHE_ALLOCATE.
3. L2 victimizes a cache line in the UC or SC state and generates a WriteEvictOrEvict transaction.

Implications

If the above conditions are met, the PE fails to increment the PMU count.

Workaround

The DSU L3 cache PMU feature can be used to count L3 allocations across all PEs in the cluster.

2058540

Incorrect Fault Status code reported for predicated SVE op

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

An SVE predicated store to a page with MTE tagging enabled that encounters a poisoned MTE Tag with no active elements and also has a tag check fail for a different MTE Tag might report a Synchronous External Abort instead of a Synchronous Tag Check Fault.

Configurations Affected

This erratum affects all configurations with the BROADCASTMTE pin asserted.

Conditions

This erratum occurs under the following conditions:

1. A PE executes an SVE predicated store to a page that is marked MTE Tagged.
2. The store accesses more than one Tag granule, such that there are no active elements corresponding to one of the granules accessed that also has a poisoned MTE tag.
3. The memory access results in a Tag check fail.

Implications

If the above conditions are met, the PE might report a Synchronous External Abort instead of Synchronous Tag Check Fault.

Workaround

This erratum has no workaround.

2061107

Tag check fail might not be reported for an unaligned predicated SVE store

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

An SVE predicated store to a page with MTE tagging enabled might not report a fault when it encounters a tag check fail.

Configurations Affected

This erratum affects all configurations with the BROADCASTMTE pin asserted

Conditions

This erratum occurs under the following conditions:

1. A PE executes an SVE predicated store to a page that is marked MTE Tagged.
2. The store access crosses a cache line boundary.
3. Both cache line accesses encounter a tag check fault.
4. Before the fault is reported, the first cache line is snooped out and another PE modifies the tag.
5. The tag check passes for the first cache line access when the line is fetched again.

Implications

If the above conditions are met, the PE might not report a Synchronous Tag Check Fault. This erratum is reported as a Programmer Category C since most of the time, a tag check fault would be correctly detected.

Workaround

This erratum has no workaround.

2089668

OSECCR_EL1/EDECCR is incorrectly included in the Warm Reset domain

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

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 CTIDEVCTL.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.

2093019

Extra A-sync packet might get written to Trace Buffer in Trace prohibited region

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, and r2p0. Fixed in r2p1.

Description

An external trace analyzer can request that an A-sync packet is injected into the trace stream, which the Embedded Trace Extension (ETE) will insert when the next P0 Element is traced. Due to this erratum, this A-sync packet might incorrectly get generated and written to trace buffer memory via TRBE under the conditions mentioned below.

Configurations Affected

This erratum affects all configurations.

Conditions

The erratum occurs under the following conditions:

1. TRBE is enabled.
2. ETE is in trace prohibited region.
3. A **TSB** instruction is executed and completed.
4. TRBE is disabled.
5. A synchronization request is received on the ATB interface.
6. TRBE is enabled.

Implications

If the above conditions occur, an A-sync packet might go to TRBE and when a new **TSB** instruction is executed, this packet might get written to memory. Under normal usage Arm expects that this unexpected trace will have no impact.

Workaround

There is no workaround.

2109742

Speculative access to a recently unmapped physical address previously containing page tables might occur

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

If the memory containing page tables is unmapped or cacheable attribute is changed while there are pending hardware prefetches to that table, the read requests might illegally occur after a DSB instruction.

Configurations Affected

All configurations are affected.

Conditions

- A table walk occurs.
- The hardware prefetcher generates a cacheable request to adjacent cache lines, allocating the L2 cache.
- The physical address containing the page tables is unmapped or cacheable attribute is changed.

Implications

If the above conditions are met, an illegal read might occur in a short window of time after the DSB instruction. Arm does not believe this will cause incorrect execution in any practical system.

Workaround

No workaround is required.

2112535

L1D_CACHE_INVALID and L2D_CACHE_INVALID PMU events fail to increment for SnpPreferUnique and SnpPreferUniqueFwd

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

When the PE receives a SnpPreferUnique or SnpPreferUniqueFwd snoop from the interconnect, it might not correctly count the L1 data cache and L2 cache invalidations that result.

Configurations Affected

This erratum affects all configurations.

Conditions

1. PE receives SnpPreferUnique or SnpPreferUniqueFwd from the coherent interconnect.
2. PE invalidates the L1 data cache and L2 cache.

Implications

If the above conditions are met, the L1D_CACHE_INVALID event will fail to increment and the L2D_CACHE_INVALID event might fail to increment. The relative infrequency of the necessary conditions means that the L1D_CACHE_INVALID and L2D_CACHE_INVALID events are still meaningful.

Workaround

There is no workaround.

2113481

MPAM value associated with instruction fetch might be incorrect

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0, r2p1. Open.

Description

Under some scenarios, the MPAM value associated with an instruction fetch request might be incorrect when context changes.

Configurations Affected

This erratum affects all configurations.

Conditions

1. An Instruction fetch request is attempted before a context switch but is not completed until after a context switch.

Implications

The MPAM value associated with the instruction fetch request might be incorrect.

Workaround

There is no workaround.

2117983

Data abort on SVE first fault load might be routed to incorrect Exception level

Status

Fault Type: Programmer Category C

Fault Status: Present in r1p0, r2p0. Fixed in r2p1.

Description

Under certain conditions, data abort on SVE first fault load might be routed to incorrect Exception level.

Configurations Affected

All configurations are affected.

Conditions

All of the following conditions must be met:

1. First active lane of SVE first fault load crosses a page boundary.
2. Translation table walk for the second page generates an external abort.
3. Memory tagging is enabled and access to bytes on the first page generates a tag check fail.
4. SCR_EL3.EA or HCR_EL2.TEA bits are set.

Implications

If the above conditions are met, data abort will not get routed to the correct Exception level. If this scenario occurred at EL0/EL1/EL2 and SCR_EL3.EA bit is set, data abort will not get routed to EL3. Likewise if this scenario occurred at EL0/EL1 and HCR_EL2.TEA bit is set and SCR_EL3.EA bit is not set, data abort will not get routed to EL2. The potential impact of this erratum to a practical system is considered to be very minor, given the precondition of an unrecoverable error.

Workaround

There is no workaround for this erratum.

2141645

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

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

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.

2143136

Some SVE PMU events count incorrectly

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

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

- 0x8074, SVE_PRED_SPEC, SVE predicated Operations speculatively executed
- 0x8075, SVE_PRED_EMPTY_SPEC, SVE predicated operations with no active predicates, Operations speculatively executed
- 0x8076, SVE_PRED_FULL_SPEC, SVE predicated operations with all active predicates, Operations speculatively executed
- 0x8077, SVE_PRED_PARTIAL_SPEC, SVE predicated operations with partially active predicates, Operations speculatively executed

Configurations Affected

This erratum affects all configurations.

Conditions

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

- 0x8074
- 0x8075
- 0x8076
- 0x8077

Implications

Load and store operations due to SVE instructions are not counted by any of these events. The counter values for these events will only reflect predicated SVE data processing operations. For example, this means that the ratios of each of the 0x8075-0x8077 event values to the 0x8074 event value will not be as expected because load and store operations are not included. However, the types of predicate used by data processing operations will still be usefully indicated.

Workaround

There is no workaround.

2146514

PMU Event MEM_ACCESS_CHECKED_WR, 0x4026 counts incorrectly and MEM_ACC_CHECKED 0x4024 might be incorrect

Status

Fault Type: Programmer Category C

Fault Status: Present in r1p0, r2p0. Fixed in r2p1.

Description

The PMU Event MEM_ACCESS_CHECKED_WR, 0x4026 does not count correctly, and MEM_ACC_CHECKED 0x4024 might not count correctly.

Configurations Affected

This erratum affects all configurations.

Conditions

1. One of the PMU event counters is configured to count event 0x4026 or 0x4024.
2. MTE is enabled.
3. SCTL_ELx.ATA=1.
4. A store instruction is executed that generates a memory-write access that is Tag Checked.

Implications

The counter values for these events will not be correct and therefore cannot be used reliably.

Workaround

There is no workaround.

2154216

FAR_ELx contents for a Data Abort exception on SVE first fault contiguous load instruction due to Tag Check fail might be incorrect

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

A SVE first fault contiguous load instruction that encounters both a Tag Check fail when accessing the first active element and a watchpoint match on one of the non-first active elements can generate a Data abort exception with an incorrect value in FAR_ELx.

Configurations Affected

All configurations are affected.

Conditions

This erratum occurs under all of the following conditions:

1. Memory tagging and watchpoints are enabled.
2. A SVE first fault contiguous load instruction accesses memory and generates a Data Abort exception due to a Tag Check fail on the first active element.
3. There is a watchpoint match on one of the non-first active elements.

Implications

If the above conditions are met, a Data Abort exception will be generated with an incorrect value in FAR_ELx. ESR_ELx will indicate Synchronous Tag Check Fault. The FAR_ELx value could be anything between the start address of the access and up to twice the access size.

Workaround

This erratum has no workaround.

2159150

Direct access of L2 data RAMs using RAMINDEX returns incomplete data

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

A direct access to the L2 data RAM using the RAMINDEX function returns incomplete data in the DDATA2 register.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following condition:

1. Direct access to internal memory targeting L2 data RAM is executed.

Implications

A direct access to the L2 data RAM will result in zeros on DDATA2_EL3[19:16]. These bits should contain ECC[15:12] corresponding to Data[127:64], but instead contains zeros.

Workaround

There is no workaround.

2174188

PMU_HOVFS event not always exported when self-hosted trace is disabled

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, and r2p0. Fixed in r2p1.

Description

PMU_HOVFS is a PMU event that can be exported to the ETM.

This event should be exported if self-hosted trace is disabled, or, if self-hosted trace is enabled and TRFCR_EL2.E2TRE == 0b1.

This event is not exported if self-hosted trace is enabled and TRFCR_EL2.E2TRE == 0b0.

Due to this erratum, when self-hosted trace is disabled, the event is never exported if TRFCR_EL2.E2TRE == 0b0.

Configurations Affected

This erratum affects all configurations.

Conditions

1. The ETM is configured to use PMU_HOVFS as an external input event.
2. Self-hosted trace is disabled and TRFCR_EL2.E2TRE == 0b0.

Implications

Overflows of PMU counters reserved by EL2 might not be visible.

Workaround

To use the PMU_HOVFS as an external input event when self-hosted trace is disabled, ensure TRFCR_EL2.E2TRE is set to 0b1.

2178034

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, r1p0, r2p0. Fixed in r2p1.

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.

2186347

64 bit source SVE PMULLB/T not considered Cryptography instruction

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

64 bit source element variants of SVE PMULLB and PMULLT are incorrectly classified as non-cryptography instructions. When the **CRYPTODISABLE** pin is asserted, 64 bit source SVE PMULLB or SVE PMULLT instructions are executed rather than taking the expected undefined instruction exception. In addition to this, when the CRYPTODISABLE pin is deasserted, PMU counts for CRYPTO_SPEC (PMU event 0x77) do not include 64 bit source SVE PMULLB and PMULLT in their counts.

Configurations Affected

This erratum affects all configurations.

Conditions

Cryptodisable

1. **CRYPTODISABLE** pin is high.
2. 64 bit source SVE PMULLB or SVE PMULLT is executed.

PMU Counts

1. **CRYPTODISABLE** pin is low.
2. PMU Enabled to count PMU EVENT 0x77 (CRYPTO_SPEC).
3. 64 bit source SVE PMULLB or SVE PMULLT is executed.

Implications

If the above conditions are met, then the instructions will be executed instead of taking the undefined exception that is required by Arm architecture.

In addition, the PMU counter for the CRYPTO_SPEC event (PMU EVENT 0x77) will not increment for 64 bit source SVE PMULLB PMULLT instructions.

Workaround

There is no workaround.

2227174

Streaming writes to memory mapped Non-shareable and write-back might cause data corruption because of reordering

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

Writes to contiguous bytes might be combined into one streaming write of 64 bytes. If such writes are performed to memory mapped Non-shareable and write-back, then two streaming writes to the same physical address might be performed in the wrong order.

Configurations Affected

This erratum affects all configurations.

Conditions

Write stream operations to memory mapped Non-shareable and write-back can allocate the L2 cache without issuing a request on the CHI interface. This creates the possibility of two concurrent pending WriteNoSnpFull transactions of the same cache line on CHI, without the proper sequencing to guarantee the order they are performed.

Implications

If the above conditions are met, then the combined writes might be performed in the wrong order as determined by the sequential execution model.

Workaround

This erratum can be avoided by mapping all write-back memory as Inner or Outer Shareable.

2238108

Read or write from Secure EL1 for ICV_BPR1_EL1 register might not work

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, and r2p0. Fixed in r2p1.

Description

Valid access to ICV_BPR1_EL1 from Secure EL1 when ICV_CTLR_EL1.CBPR is set to 1 should modify ICV_BPRO_EL1 on writes and return the value from ICV_BPRO_EL1 on reads. Instead, reads of ICV_BPR1_EL1 return ICV_BPRO_EL1 plus one, saturated to 0b111. Writes to ICV_BPR1_EL1 are ignored.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. The PE is in Secure state in the EL1 exception level.
2. ICV_CTLR_EL1.CBPR is set to 1.
3. A valid read or write access to ICV_BPR1_EL1 occurs.

Implications

If the above conditions are met, then an incorrect value might be returned on read or a valid write might be ignored potentially, affecting the priority of interrupts in the CPU.

Workaround

This erratum has no workaround.

2238111

Reads of DISR_EL1 incorrectly return 0s while in Debug State

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

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.

2239139

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

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

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 UNDEFINED instruction.

Workaround

There is no workaround.

2243871

ELR_ELx[63:48] might hold incorrect value when PE disables address translation

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

When the CPU executes an exception return in order to switch context and the new context satisfies certain rare conditions, the top 16 bits of ELR_ELx might track an incorrect value.

Configurations Affected

The erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. CPUACTLR_EL1[22] is set to 1.
2. The PE executes an ERET, ERETAA or ERETAB instruction to switch to a new context.
3. Either stage 1 or stage 2 translation was enabled when ERET is executed. After ERET, both stage 1 and stage 2 translations are turned off.
4. ELR_ELx[63:48] specified by ERET is neither 0x0000 (all zero) nor 0xffff (all one).

Implications

When the above conditions are met, the PE takes instruction abort (address size fault) or asynchronous exception after ERET without executing the instruction in the context specified by ERET. After the exception is taken, ELR_ELx specified by ERET should hold the same value because no instruction is executed. However, PE might modify ELR_ELx[63:48] to zero.

ERET with non-zero ELR_ELx[63:48] causes an address size fault during address translation disabled because the CPU supports less than 256TB physical address space. Arm also assumes the new context is controlled by privileged software (for example, Hypervisor) because translation is turned off. Therefore, software can hit this erratum only when the system software uses this malicious address in the ELR_ELx register.

Workaround

This erratum has no workaround.

2245716

TRBE might use incorrect Cacheability attributes for TRBE data when address translation is disabled

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

Under certain conditions, Trace Buffer Extension (TRBE) might use incorrect Cacheability attributes for TRBE data when address translation is disabled.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. TRBE is enabled with `TRBLIMITR_EL1.nVM == 1`.
2. `TRBMAR_EL1.Attr` is programmed to use Cacheable attributes.
3. `MDCR_EL2.E2TB = 2'b00` (EL2 owning)
4. `HCR_EL2.CD=1` and `HCR_EL2.VM=1`
5. PE is executing at EL=1 or EL=0.
6. TRBE writes data to memory.

Implications

When the above conditions are met, PE might incorrectly use Non-Cacheable attribute instead of Cacheable attribute from `TRBMAR_EL1.Attr[3:0]` for TRBE data. Trace data might be lost if the memory location used by TRBE is present in cache when this write happens.

Workaround

This erratum has no workaround.

2245832

ESR_ELx contents for a Data Abort exception might be incorrect when an L1D tag double bit error is encountered

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

When an L1D tag double bit error is encountered, a Data Abort exception might be reported with an incorrect fault type of Synchronous Tag Check Fault in the ESR_ELx register under unusual micro architectural conditions.

Configurations Affected

This erratum affects all configurations with the BROADCASTMTE pin asserted.

Conditions

This erratum occurs under all of the following conditions:

1. Memory tagging is enabled.
2. A precise checked access due to a load instruction encounters L1D tag double bit error.

Implications

If the previous conditions are met, a Data Abort exception will be generated with an incorrect Data Fault Status Code (DFSC) of Synchronous Tag Check Fault in the ESR_ELx register when it should have been Synchronous External Abort.

If this scenario occurred at EL0/EL1/EL2 and SCR_EL3.EA bit is set, then Data Abort will not get routed to EL3.

Likewise if this scenario occurred at EL0/EL1 and HCR_EL2.TEA bit is set, then Data Abort will not get routed to EL2. A fatal RAS error will still be reported.

Workaround

This erratum has no workaround.

2247178

L1 MTE Tag poison is not cleared

Status

Fault Type: Programmer Category C
Fault Status: Present in r1p0, r2p0. Fixed in r2p1.

Description

The MTE Tag poison is not cleared by an STG or DC G[Z]VA instruction.

Configurations Affected

This erratum affects all configurations with the BROADCASTMTE pin asserted.

Conditions

This erratum occurs under the following conditions:

1. A Processing Element (PE) accesses a line that encounters poison on the MTE Tag.
2. The PE executes an STG or DC G[Z]VA to the same 16-byte address.

Implications

If the above conditions are met, then the MTE Tag poison does not get cleared in the L1 Tag.

Workaround

There is no workaround.

2254450

L1 Data poison is not cleared by a store

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

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.

2276444

PMU event for full/partial/empty/not full predicate incorrect for some SVE instructions

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

The PMU events for full/partial/empty/not full predicate capture the cases where an instruction reads a full, not full, partial, or empty value for governing predicate, according to the size of the instruction. Under certain circumstances, the event might be incorrectly captured.

Configurations Affected

This erratum affects all configurations.

Conditions

- PMU is configured to sample events for SVE_PRED_EMPTY_SPEC (0x8075), SVE_PRED_FULL_SPEC (0x8076), SVE_PRED_NOT_FULL_SPEC (0x8079), or SVE_PRED_PARTIAL_SPEC (0x8077).
- One of these SVE conversion instructions is executed: SCVTF, UCVTF, FCTVZU, FCVTZS, FCVT, FCVTX, FCVTXNT, or FCVTNT.
- Governing predicate used by instruction has a different value than All-Active or All-Empty.

Implications

If the previous conditions are met, the following events might be incorrectly captured:

- PMU event SVE_PRED_EMPTY_SPEC (0x8075)
- PMU event SVE_PRED_FULL_SPEC (0x8076)
- PMU event SVE_PRED_NOT_FULL_SPEC (0x8079)
- PMU event SVE_PRED_PARTIAL_SPEC (0x8077)

Workaround

This erratum has no workaround.

2278134

PMU L1D_CACHE_REFILL_OUTER is inaccurate

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

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.

2283666

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, r1p0, and r2p0. Fixed in r2p1.

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.

2307829

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, r1p0, r2p0. Fixed in r2p1.

Description

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

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following condition:

- Data double bit error or external abort is encountered during translation table walk and synchronous exception is reported.

Implications

If the previous conditions are met, ESR_ELx.ISV bit will be set.

Workaround

This erratum has no workaround.

2317617

ESR_ELx contents for a Data Abort exception might be incorrect when a data double bit error or external abort is encountered

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, and r2p0. Fixed in r2p1.

Description

When a data double bit error or external abort is encountered on one half of an unaligned load, a Data Abort exception might be reported with an incorrect fault type of Synchronous Tag Check Fault in the ESR_ELx register. This occurs under unusual micro-architectural conditions.

Configurations Affected

This erratum affects all configurations with the BROADCASTMTE pin asserted.

Conditions

This erratum occurs under all of the following conditions:

1. Memory tagging is enabled.
2. A precise checked access due to an unaligned load instruction encounters a data double bit error or external abort.

Implications

If the previous conditions are met, a Data Abort exception will be generated with an incorrect Data Fault Status Code (DFSC) of Synchronous Tag Check Fault in the ESR_ELx register, when it should have been Synchronous External Abort.

If this scenario occurred at EL0/EL1/EL2, and the SCR_EL3.EA bit is set, then the Data Abort will not get routed to EL3.

Likewise, if this scenario occurred at EL0/EL1, and the HCR_EL2.TEA bit is set, then the Data Abort will not get routed to EL2. A RAS error will still be reported.

Workaround

This erratum has no workaround.

2334390

L2 tag RAM double-bit ECC error might lead to the PE not responding to a forwarding snoop

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, and r2p0. Fixed in r2p1.

Description

A double-bit ECC error in a cache line containing Memory Tagging Extensions (MTE) tags might result in the L1 and L2 caches becoming out-of-sync with respect to MTE tag validity. This can lead to a situation in which the L1 evicts dirty MTE tags to the L2 as part of a fill/evict sequence or a snoop. If this eviction satisfies an external forwarding snoop, the RN-F might fail to provide legal responses which might lead to a deadlock.

Configurations Affected

This erratum affects all configurations using the Memory Tagging Extensions.

Conditions

When using MTE, under specific microarchitectural and timing conditions, an L2 double-bit ECC error in the L2 tag RAMs might allow the L1 data cache to later evict a cache line with dirty MTE tags. The erratum occurs if the eviction satisfies an external snoop of one of these types:

- SnpUniqueFwd
- SnpCleanFwd
- SnpSharedFwd
- SnpNotSharedDirtyFwd
- SnpPreferUniqueFwd

Implications

If the previous conditions are met, the PE might provide an SnpRespDataFwded response to the HN-F, but fail to provide a CompData response to the original requester, leading to a system deadlock.

Workaround

This erratum has no workaround.

2344960

CSSELR_EL1.TnD is RAZ/WI when CSSELR_EL1.InD == 0x1

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, and r2p0. Fixed in r2p1.

Description

In some contexts when CSSELR_EL1.InD == 0x1, CSSELR_EL1.TnD is defined to be RES0.

In other contexts when CSSELR_EL1.InD == 0x0, CSSELR_EL1.TnD is defined to be R/W.

When a bit is RES0 in some contexts and R/W in other contexts, then it cannot be implemented as RAZ/WI for RES0 contexts.

In affected products, CSSELR_EL1.TnD is incorrectly treated as RAZ/WI instead of the correct R/W behavior when CSSELR_EL1.InD == 0x1.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. The PE is executing with CSSELR_EL1.InD == 0x1.
2. The PE attempts to read or write CSSELR_EL1.TnD.

Implications

Reads of CSSELR_EL1.TnD will return 0x0 and writes will be ignored.

Workaround

This erratum is not expected to require a workaround.

2382765

Incorrect read value for Performance Monitors Configuration Register

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0. Fixed in r2p1.

Description

The external register Performance Monitors Configuration (PMCFGR) returns an incorrect read value for the following field in the register:

- CCD

Configurations Affected

This erratum affects all configurations.

Conditions

1. Debugger reads the PMCFGR register.

Implications

The register field PMCFGR.CCD incorrectly reads as 0b1, indicating that Cycle counter has prescale. The expected value is 0b0, since Aarch32 isn't supported.

Workaround

There is no workaround.

2391680

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, r1p0, r2p0, and r2p1. 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.

2444421 PMU STALL_SLOT_BACKEND and STALL_SLOT_FRONTEND events count incorrectly

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0, and r2p1. 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.

2643627

ERXPFGCDN_EL1 register is incorrectly written on Warm reset

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r1p0, r2p0, and r2p1. Open.

Description

The ERXPFGCDN_EL1 register is written a reset value of 0 at both cold and Warm reset, when it should only be reset at Cold reset.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs when a Warm reset occurs.

Implications

If the previous condition is met, the value of ERXPFGCDN_EL1 will not be preserved across a Warm reset.

Workaround

This erratum has no workaround.

2647274

Incorrect read value for Performance Monitors Control Register

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0 and r2p1. Open.

Description

The Performance Monitors Control Register (PMCR_ELO) 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_ELO.X, or debugger writes a nonzero value to the PMCR.X
2. Software reads the PMCR_ELO 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.

2652240

FAR_ELx contents for a Data Abort exception on SVE first fault contiguous load instruction due to Tag Check fail might be incorrect

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0, r2p1. Open.

Description

A *Scalable Vector Extension* (SVE) first fault contiguous load instruction that encounters a Tag Check fail when accessing the first active element and a watchpoint match on one of the non-first active elements can generate a Data abort exception with incorrect value in FAR_ELx.

Configurations Affected

All configurations are affected.

Conditions

This erratum occurs under all of the following conditions:

1. Memory tagging and watchpoints are enabled.
2. An SVE first fault contiguous load instruction accesses memory and generates a Data Abort exception due to Tag Check fail on the first active element.
3. There is a watchpoint match on one of the non-first active elements.

Implications

If the above conditions are met, a Data Abort exception will be generated with an incorrect value in FAR_ELx. ESR_ELx will indicate Synchronous Tag Check Fault.

Workaround

This erratum has no workaround.

2676362

Execution of STG instructions in close proximity might cause loss of MTE allocation tag data

Status

Fault Type: Programmer Category C

Fault Status: Present in r1p0, r2p0, r2p1. Open.

Description

Under certain rare micro-architectural conditions, two or more STG instructions that access the same cacheline but different 32-bytes might not write the *Memory Tagging Extension* (MTE) allocation tag to memory in the presence of an ECC error to the same cache index.

Configurations Affected

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

Conditions

This erratum occurs under the following conditions:

1. Memory tagging is enabled.
2. Two or more STG instructions are executed in close proximity to the same cache line.
3. The STG instructions access different 32-bytes locations.
4. An L2 fill for a different cacheline but to the same index has a single bit data error that could have otherwise caused a capacity evict of the cacheline accessed by the STG instructions.

Implications

If the above conditions are met, then under specific micro-architectural conditions, the MTE allocation tag might not be written to memory, resulting in a silent corruption of the MTE tag.

Workaround

If desired, this erratum can be avoided by setting CPUACTLR5_EL1[13] to 1.

Note: setting CPUACTLR5_EL1[13] to 1 is expected to result in a small performance degradation for workloads that use MTE (approximately 1.6% when using MTE imprecise mode, 0.9% for MTE precise mode).

2692441

L3D PMU events may be inaccurate

Status

Fault Type: Programmer Category C

Fault Status: Found in r0p0, r1p0, r2p0, r2p1. Open.

Description

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

- 0x0029 L3D_CACHE_ALLOCATE
- 0x002a L3D_CACHE_REFILL
- 0x002b L3D_CACHE
- 0x00a0 L3D_CACHE_RD
- 0x400B L3D_CACHE_LMISS_RD

Configurations Affected

This erratum affects all configurations.

Conditions

No specific conditions are needed for this erratum to occur.

Implications

The following events might be over or under-counted:

- L3D_CACHE_ALLOCATE
- L3D_CACHE_REFILL
- L3D_CACHE
- L3D_CACHE_RD
- L3D_CACHE_LMISS_RD

Workaround

Use equivalent PMU counters in the L3 cache. Note that the L3 cache PMU counters will represent activity for all Processing Elements (PEs) in the DSU cluster.

2694769

MTE checked load might read an old value of allocation tag by not complying with address dependency ordering

Status

Fault Type: Programmer Category C

Fault Status: Present in r1p0, r2p0, r2p1. Open.

Description

Under some unusual micro-architectural conditions, checked load might read an old value of allocation tag by not complying with address dependency ordering.

Configurations Affected

All configurations are affected.

Conditions

The erratum occurs when all the following apply:

1. Initially, memory location M has allocation tag A.
2. Processing Element x (PE_x) stores to M using allocation tag A.
3. PE_y changes the allocation tag of M from A to B.
4. PE_x makes a checked load from M using allocation tag A, with a dependency such that it should observe allocation tag B.

Implications

If the above conditions are met, PE_x may not observe the new allocation tag for the memory location and may fail to report a tag check fail.

Workaround

This erratum has no workaround.

2712632

Incorrect read value for Performance Monitors Configuration Register EX field

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0, r2p1. 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.

2726256

IRG instructions might produce the wrong tag when GCR_EL1.RRND=0x0.

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0 and r2p1. Open.

Description

When the *Processing Element* (PE) is configured with GCR_EL1.RRND=0x0, writing SCTLR_EL3.ATA, SCTLR_EL2.ATA, SCTLR_EL1.ATA, or SCTLR_EL1.ATA0 can corrupt internal state. As a result IRG instructions might produce the wrong tag.

Configurations Affected

This erratum affects all configurations with MTEDISABLE=0x0.

Conditions

This erratum occurs under the following conditions:

1. The PE is executing with GCR_EL1.RRND=0x0.
2. An IRG instruction is executed.
3. An MSR is executed which updates any of SCTLR_EL3.ATA, SCTLR_EL2.ATA, SCTLR_EL1.ATA, or SCTLR_EL1.ATA0.
4. An IRG instruction is executed.

Implications

If the above conditions are met, the tag produced by the second or any subsequent IRG instruction might be incorrect.

Workaround

Arm is not aware of any software which uses the GCR_EL1.RRND=0x0 configuration. If your system uses this configuration, please contact Arm Customer Support for more information.

2769023

STALL_BACKEND_MEM, Memory stall cycles AMU event count incorrectly

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0, and r2p1. Open.

Description

The following *Activity Monitor Unit* (AMU) event does not count correctly:

- 0x4005, STALL_BACKEND_MEM. The counter counts cycles in which the PE is unable to dispatch instructions from the frontend to the backend of the PE. It is due to a backend stall caused by a miss in the last level of cache within the PE clock domain. This event is counted by AMEVCNTR03.

Configurations Affected

This erratum affects all configurations.

Conditions

- AMU is enabled

Implications

The counter values for the event will not be correct and therefore cannot be used reliably.

Workaround

This erratum has no workaround.

2798805

Incorrect decoding of SVE version of PRF* scalar plus scalar instructions

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0, r2p1. Open.

Description

Scalar plus Scalar forms of the *Scalable Vector Extension* (SVE) PRF may not prefetch from the correct address. The address should be $X_n + X_m \ll \text{scalar}$, but is instead calculated as X_n . This affects the following instructions:

- PRFB (scalar plus scalar)
- PRFH (scalar plus scalar)
- PRFW (scalar plus scalar)
- PRFD (scalar plus scalar)

Configurations Affected

This erratum affects all configurations.

Conditions

1. Any of the above instructions are executed without trapping when $X_m \neq 0x0$

Implications

All affected instructions are software prefetches which do not affect architectural state in any way (including suppression of any translation faults). Thus this erratum will not affect the functional operation of the CPU. Since these instructions are likely to be used in contexts where X_n is fixed and X_m is incrementing, it is unlikely that the erroneous prefetches would result in undesired cache pollution or reduction in memory bandwidth because the instructions will simply continuously prefetch the same address.

Workaround

No workaround is expected to be necessary, but if one is specifically needed, the programmer can use an ADD, and then one of the immediate forms of SVE PRF, which are unaffected. These instructions are:

- PRFB (scalar plus immediate)
- PRFH (scalar plus immediate)

- PRFW (scalar plus immediate)
- PRFD (scalar plus immediate)

2799687

ECC errors in MTE allocation tags may lead to silent data corruption in tag values

Status

Fault Type: Programmer Category C

Fault Status: Present in r1p0, r2p0, and r2p1. Open.

Description

Streaming writes that require *Memory Tagging Extension* (MTE) tags for tag checking or merging with data receive allocations tags that are flagged as poisoned may lead to the *Processing Element* (PE) caching data and tags with no indication that the tags are poisoned. This may lead to silent data corruption on the allocation tags.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. The PE performs a streaming write (a write of 64 contiguous bytes gathered from multiple store or DC ZVA operations).
2. Streaming write requires MTE tag check or hits in the PE caches to a line that contains MTE allocation tags.
3. MTE allocations tags contain an indication of an error (uncorrectable ECC error or poison flag).

Implications

If the above conditions are met, the PE might merge the streaming write data and the MTE allocation tags containing an error and write data and allocation tags to a cache without marking the tags as poisoned. This can lead to silent data corruption to future consumers of the MTE allocation tags, which may result in incorrect MTE tag check results. The net effect is an increase in the SDC FIT rate of the PE.

There is still substantial benefit being gained from the ECC logic.

Workaround

There is no workaround.

2814414

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

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0, r2p1. Open.

Description

The timestamp value that is captured in the *Statistical Profiling Extension* (SPE) records may be incorrect.

Configurations Affected

This erratum affects all configurations.

Conditions

1. Timestamp capture is enabled for SPE records at the appropriate Exception level 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 stale (off by one tick) or zero in some cases.

Workaround

There is no workaround.

2814418

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, r1p0, r2p0, and r2p1. 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.

2817889

TRBE buffer write translation out of context may have incorrect memory attributes

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0, and r2p1. Open.

Description

When `TRBLIMITR_EL1.nVM = 1`, `TBE_OWNING_EL = EL1`, and TRBE requests a translation while the *Processing Element* (PE) is executing in EL2 or EL3, and cache is disabled by `HCR_EL2.CD = 1`, memory attribute may not be Non-cacheable.

Configurations affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. `TRBLIMITR_EL1.nVM` is set to 1.
2. `MDCR_EL2.E2TB` is set to 0b10 or 0b11.
3. `HCR_EL2.CD` is set to 1.
4. The PE is executing in EL2 or EL3.
5. TRBE requests a translation for a buffer write.

Implications

Memory attributes for any write access by TRBE to that translation may not be forced to Non-cacheable.

Workaround

Use of `HCR_EL2.CD` is not expected to be common. If a workaround is needed, do not allow TRBE to be given to a VM machine.

2910963

L2D_CACHE_WB_CLEAN overcounts

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r1p0, r2p0 and r2p1. Open.

Description

Counting of the L2D_CACHE_WB_CLEAN event includes transfer of data directly to another *Processing Element* (PE) using the AMBA CHI Direct Cache Transfer mechanism.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. The PE processes a forwarding snoop from the DSU or Fully coherent Home Node (HN-F) and sends data directly to another PE using a CompData message.

Implications

If the previous condition is met, the PE will count the L2D_CACHE_WB_CLEAN event contrary to the architectural specification of this event.

Workaround

No workaround is required for this erratum.

2921487

Accessing a memory location using mismatched Shareability attributes when MTE tag checking is enabled might cause data corruption

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0 and r2p1. Open.

Description

A PE accessing a same physical memory location with mismatched Shareability attributes and requiring a read of *Memory Tagging Extension* (MTE) tags might result in data corruption.

Configurations Affected

This erratum affects all configurations.

Conditions

This erratum occurs under the following conditions:

1. PE accesses a physical memory location using cacheable and Non-shareable attributes.
2. PE accesses the same physical address using cacheable and shareable attributes with MTE checking enabled.

Implications

If the previous conditions are met, the PE might expose stale data from the PE caches established by a Non-shareable access. This data might become visible to shareable observers in the same Shareability domain, even if the PE performs the required cache maintenance for ensuring ordering and coherency when aliasing Shareability.

Workaround

Arm expects that operating systems do not use mismatched Shareability attributes for aliases of the same memory location for tagged pages.

3061569

TagMatch responses with error indication do not generate a SError abort

Status

Fault Type: Programmer Category C

Fault Status: Present in r0p0, r1p0, r2p0, and r2p1. Open.

Description

When tag checks are performed outside of the *Processing Element* (PE), the AMBA CHI protocol returns a TagMatch response that indicates whether or not the tag check succeeded or failed. If an error condition occurred while performing the tag check, the system might return the TagMatch response with an error indication. If this occurs, the PE should report a SError abort, but fails to do so.

Configurations affected

This erratum affects all configurations with the BROADCASTMTE pin asserted.

Conditions

This erratum occurs under the following conditions:

1. PE has *Memory Tagging Extension* (MTE) enabled in asynchronous checking of stores.
2. PE performs tag checked stores.
3. Write streaming causes the PE to send the stores to the interconnect as write transactions.
4. While performing the tag check operation for the write, the interconnect encounters an error condition while reading the tag value.

Implications

If the conditions are met, the interconnect might return a TagMatch response with an error indication, but the PE might not generate a SError abort. If the TagMatch response indicates a tag check failure (Resp=Fail), TFSR_ELx bits will still be updated.

Workaround

No workaround is required for this erratum.

