Arm® Neoverse CMN S3 (AE) Coherent Mesh Network

Software Developer Errata Notice

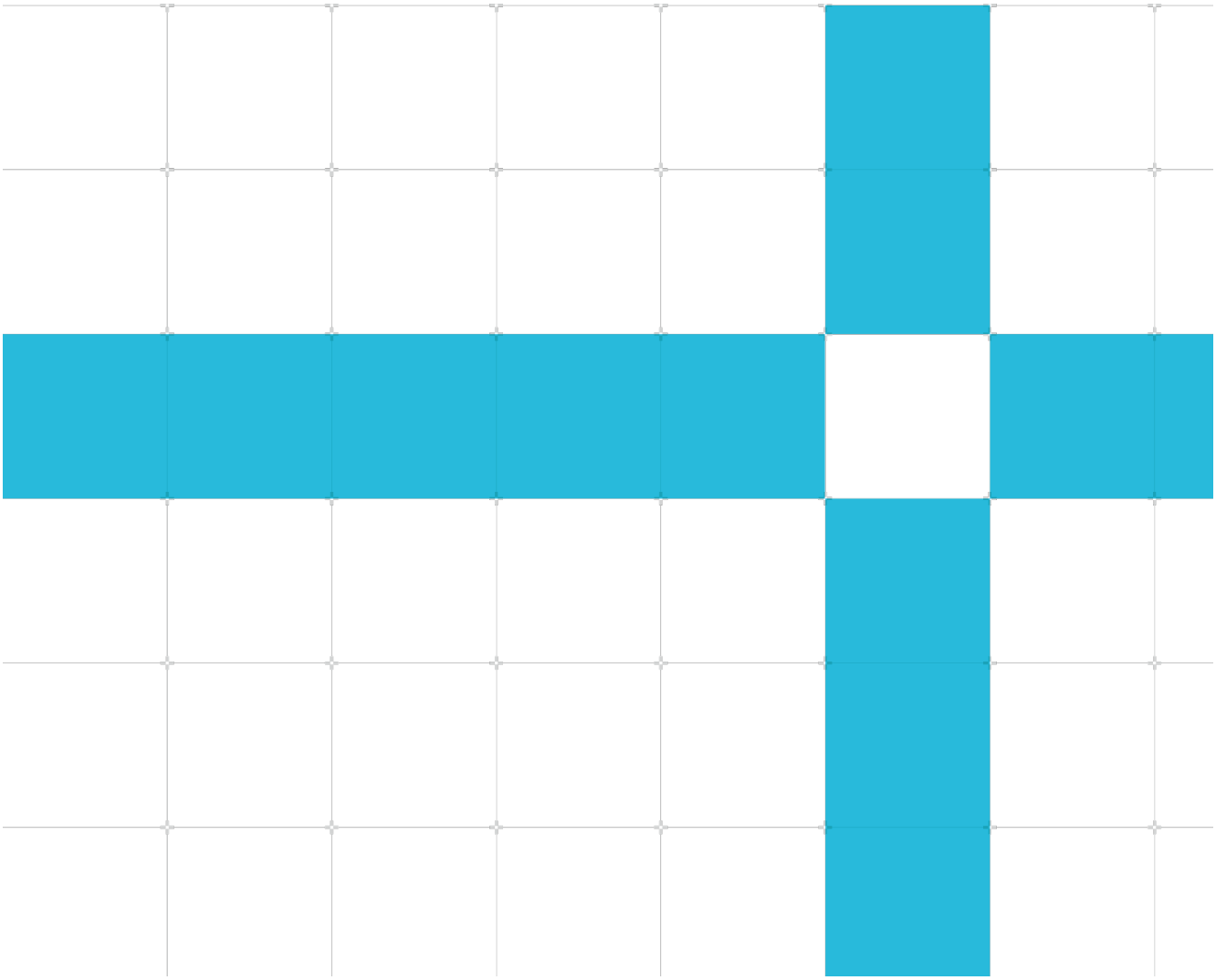
Date of issue: February 07, 2025

Non-Confidential

Document version: 12.0

Document ID: SDEN-2904806

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



This document (SDEN_2904806_12.0_en) was issued on February 07, 2025.

There might be a later issue at **http://developer.arm.com/documentation/SDEN-2904806**

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**.

Feedback

Arm welcomes feedback on this product and its documentation. To provide feedback on Arm® Neoverse CMN S3 (AE) Coherent Mesh Network, 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**.

Contents

Introduction

Scope

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

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

Categorization of errata

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

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

Change Control

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

February 07, 2025: Changes in document version v12.0

No new or updated errata in this document version.

February 06, 2025: Changes in document version v11.0

No new or updated errata in this document version.

October 29, 2024: Changes in document version v10.0

ID	Status	Area	Category	Summary
3363760	Updated	Programmer	Category B	A continuous stream of DVM Operations requests by Peer DN and Remote chip requestors can starve Local DVM Syncs
3606070	Updated	Programmer	Category B	CCG CXL3.0 receiver does not support late poison
3355767	Updated	Programmer	Category C	Incorrect MXP RAS ERRSRC logging information
3625665	Updated	Programmer	Category C	HN-S RAS Overflow INTREQ not asserted on first Correctable Error after writing 0xFFFF to Correctable Error Counter

July 26, 2024: Changes in document version v9.0

ID	Status	Area	Category	Summary
3606070	New	Programmer	Category B	CCG CXL3.0 receiver does not support late poison
3625665	New	Programmer	Category C	HN-S RAS Overflow INTREQ not asserted on first Correctable Error after writing 0xFFFF to Correctable Error Counter

June 12, 2024: Changes in document version v8.0

ID	Status	Area	Category	Summary
3223098	New	Programmer	Category B	RN-I/RN-D can return same ARID reads out of order when AXI data interleaving is disabled
3363760	New	Programmer	Category B	A continuous stream of DVM Operations requests by Peer DN and Remote chip requestors can starve Local DVM Syncs
3355767	New	Programmer	Category C	Incorrect MXP RAS ERRSRC logging information

March 28, 2024: Changes in document version v7.0

ID	Status	Area	Category	Summary
3189964	New	Programmer	Category B	More than two XY route override can result in deadlocks
3245612	New	Programmer	Category B	Incorrect SDC multi-cycle path constraints for 2xREQ configurations
2958415	Updated	Programmer	Category C	System Level Cache cache lines in locked way can be evicted
2964003	Updated	Programmer	Category C	Incorrect Correctable Error Logging in HN-S and HN-F components
2976084	Updated	Programmer	Category C	Debug reads with simultaneous coherent traffic or dynamic power transitions can cause deadlock
3217599	New	Programmer	Category C	HN-S Non-Secure, Root, or Realm RAS events may be reported in Secure error records
3283582	New	Programmer	Category C	On-Chip Memory Mode entrance and exit can result in data inconsistency

December 05, 2023: Changes in document version v6.0

ID	Status	Area	Category	Summary
3021108	New	Programmer	Category B	A continuous stream of DVM Operations requests by Peer DN and Remote chip requestors can starve Local DVM Operations
3105737	New	Programmer	Category C	Incorrect MPAM_MSMON_IDR value for NO_HW_OFLW_INTR bit [30]

October 31, 2023: Changes in document version v5.0

ID	Status	Area	Category	Summary
3038872	Updated	Programmer	Category A	Multi-chip SMP deadlock in the presence of CPU traffic when CCG HA_REQ_PASS_BUFF_DEPTH < RA_NUM_REQS
2982880	Updated	Programmer	Category B	Write stashes can cause multi-copy atomicity issue
3031171	Updated	Programmer	Category B	QoS QPC can be corrupted in 2xREQ configurations
3033427	Updated	Programmer	Category B	CCG might not service IDE stop on the CXS interface
3043435	New	Programmer	Category B	Snoop Filter flush does not propagate Persistent CMO when FORCE_FLUSH_PCMO_EN is set
3085420	New	Programmer	Category B	MPAM CSU Monitors may capture incorrect values
2985283	Updated	Programmer	Category B (rare)	Incorrect TagMatch response on partial writes with MTE Match
3066481	New	Programmer	Category B (rare)	Dirty Memory Tag Extension tags can be dropped in On-Chip Memory mode
2976084	Updated	Programmer	Category C	Debug reads with simultaneous coherent traffic or dynamic power transitions can cause deadlock

September 15, 2023: Changes in document version v4.0

ID	Status	Area	Category	Summary
3038872	New	Programmer	Category A	Multi-chip SMP deadlock in the presence of CPU traffic when CCG HA_REQ_PASS_BUFF_DEPTH < RA_NUM_REQS
3031171	Updated	Programmer	Category B	QoS QPC can be corrupted in 2xREQ configurations
3033427	New	Programmer	Category B	CCG might not service IDE stop on the CXS interface

August 24, 2023: Changes in document version v3.0

ID	Status	Area	Category	Summary
2982880	New	Programmer	Category B	Write stashes can cause multi-copy atomicity issue
3031171	New	Programmer	Category B	QoS QPC can be corrupted in 2xREQ configurations
2985283	New	Programmer	Category B (rare)	Incorrect TagMatch response on partial writes with MTE Match
2958415	New	Programmer	Category C	System Level Cache cache lines in locked way can be evicted
2976084	New	Programmer	Category C	Debug reads with simultaneous coherent traffic or dynamic power transitions can cause deadlock

August 01, 2023: Changes in document version v2.0

ID	Status	Area	Category	Summary
2964003	New	Programmer	Category C	Incorrect Correctable Error Logging in HN-S and HN-F components

March 27, 2023: Changes in document version v1.0

No errata in this document version.

Errata summary table

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

ID	Area	Category	Summary	Found in versions	Fixed in version
3038872	Programmer	Category A	Multi-chip SMP deadlock in the presence of CPU traffic when CCG HA_REQ_PASS_BUFF_DEPTH < RA_NUM_REQS	r0p0	r0p1
2982880	Programmer	Category B	Write stashes can cause multi-copy atomicity issue	r0p0	r0p1
3021108	Programmer	Category B	A continuous stream of DVM Operations requests by Peer DN and Remote chip requestors can starve Local DVM Operations	r0p0	r0p1
3031171	Programmer	Category B	QoS QPC can be corrupted in 2xREQ configurations	r0p0	r0p1
3033427	Programmer	Category B	CCG might not service IDE stop on the CXS interface	r0p0	r0p1
3043435	Programmer	Category B	Snoop Filter flush does not propagate Persistent CMO when FORCE_FLUSH_PCMO_EN is set	r0p0	r0p1
3085420	Programmer	Category B	MPAM CSU Monitors may capture incorrect values	r0p0	r0p1
3189964	Programmer	Category B	More than two XY route override can result in deadlocks	r0p0, r0p1	r1p0
3223098	Programmer	Category B	RN-I/RN-D can return same ARID reads out of order when AXI data interleaving is disabled	r0p0, r0p1	r1p0
3245612	Programmer	Category B	Incorrect SDC multi-cycle path constraints for 2xREQ configurations	r0p0, r0p1	r1p0
3363760	Programmer	Category B	A continuous stream of DVM Operations requests by Peer DN and Remote chip requestors can starve Local DVM Syncs	r0p0, r0p1, r1p0	r2p0
3606070	Programmer	Category B	CCG CXL3.0 receiver does not support late poison	r0p0, r0p1, r1p0	r2p0
2985283	Programmer	Category B (rare)	Incorrect TagMatch response on partial writes with MTE Match	r0p0	r0p1
3066481	Programmer	Category B (rare)	Dirty Memory Tag Extension tags can be dropped in On-Chip Memory mode	r0p0	r0p1

ID	Area	Category	Summary	Found in versions	Fixed in version
2958415	Programmer	Category C	System Level Cache cache lines in locked way can be evicted	r0p0, r0p1	r1p0
2964003	Programmer	Category C	Incorrect Correctable Error Logging in HN-S and HN-F components	r0p0, r0p1	r1p0
2976084	Programmer	Category C	Debug reads with simultaneous coherent traffic or dynamic power transitions can cause deadlock	r0p0, r0p1	r1p0
3105737	Programmer	Category C	Incorrect MPAM_MSMON_IDR value for NO_HW_OFLW_INTR bit [30]	r0p0	r0p1
3217599	Programmer	Category C	HN-S Non-Secure, Root, or Realm RAS events may be reported in Secure error records	r0p0, r0p1	r1p0
3283582	Programmer	Category C	On-Chip Memory Mode entrance and exit can result in data inconsistency	r0p0, r0p1	r1p0
3355767	Programmer	Category C	Incorrect MXP RAS ERRSRC logging information	r0p0, r0p1, r1p0	r2p0
3625665	Programmer	Category C	HN-S RAS Overflow INTREQ not asserted on first Correctable Error after writing 0xFFFF to Correctable Error Counter	r0p0, r0p1, r1p0	r2p0

Errata descriptions

Category A

3038872
Multi-chip SMP deadlock in the presence of CPU traffic when CCG HA_REQ_PASS_BUFF_DEPTH < RA_NUM_REQS

Status

Affects: CMN S3
Fault Type: Programmer Cat-A
Fault Status: Present in r0p0. Fixed in r0p1.

Description

High-bandwidth CPU traffic targeting a remote chip can result in deadlocks.

Configurations Affected

All configurations where a CCG node on one side of the CML_SMP link has a HA_REQ_PASS_BUFF_DEPTH value less than the RA_NUM_REQS value of the CCG node on the other side of the CML_SMP link.

Conditions

High bandwidth CPU traffic targeting the remote chip.

Implications

Deadlocks in the presence of CPU traffic.

Workaround

No workarounds.

Category A (rare)

There are no errata in this category.

Category B

2982880
Write stashes can cause multi-copy atomicity issue

Status

Affects: CMN S3
Fault Type: Programmer Cat-B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

CHI and AXI Write Stash operations can incorrectly get early completion before snooping is complete causing multi-copy atomicity issues.

For example, an RN-I or RN-D PCI MSI write issued after a Write Stash can result in the CPU having the older or stale copy of the Write Stash data at the time of the MSI interrupt.

Another example is an RN-I or RN-D write flag issued after completion of the Write Stash, the CPU can observe the flag update before the Write Stash data is updated.

Note that Arm CPUs do not issue Write Stash transactions.

Configurations affected

Any CMN configuration.

Conditions

This erratum occurs when the following conditions are met:

- RN-I or RN-D issues AXI Write Stash transaction with a valid StashNID targeting a CPU cache
- RN-I or RN-D issues another AXI transaction after receiving the completion for the Write Stash. For example, PCIE MSI write or write to flag address
- The Stash CPU can observe the results of the second transaction above before the Write Stash data is updated for the first

Implications

If the conditions are met, Write Stash might receive early completion while the Stash CPU still has old copy causing multi-copy atomicity issues.

Workarounds

Use the following workaround to send the result in Stash to the SLC instead of the CPU cache, by disabling stash snooping using cmn_hns_cfg_ctl.stash_snp_dis.

3021108
A continuous stream of DVM Operations requests by Peer DN and Remote chip requestors can starve Local DVM Operations

Status

Affects: CMN S3
Fault Type: Programmer Cat-B
Fault Status: Present in r0p0. Fixed in: r0p1

Description

In multi-chip SMP with multi-DVM domain configurations, a DVM Node (DN) that receives a constant stream of DVM Operation (DVMOp) requests from a remote chip and Peer DN (PDN) requestors can result in local DVMOp requests being starved.

Configurations affected

Multi-chip SMP configurations with multiple DVM domains per chip.

Conditions

This erratum occurs if all the following conditions are met:

- DVM domains are configured to receive DVM requests from both remote chips and PDNs.
- RN-Fs in the PDN's domain and remote chip send a continuous stream of DVMOps. For example, TLB Invalidate operations resulting a DN receiving a continuous stream of DVMOps from the PDN and remote chip(s).
- The same DN receives DVM request from its local RN-Fs.

Implications

If the above conditions are met, the DVMOps sent from local RN-Fs might not complete, resulting in a deadlock.

Workaround

Configure CMN to a single DN domain using the boot-time software configuration. For details on DN domain configuration, see the Arm® Neoverse™ CMN S3 Technical Reference Manual.

3031171
QoS QPC can be corrupted in 2xREQ configurations

Status

Affects: CMN S3
Fault Type: Programmer Cat-B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

The QoS QPC value can be corrupted in 2xREQ configurations. The QPC value can be overridden to zero depending on the location of the RN-F, RN-I, RN-D, HN-F or CCG device within the mesh.

Configurations affected

Configurations with 2xREQ.

Conditions

This erratum occurs when all the following conditions are met:

- The RN-F (pass-through mode only), RN-I, RN-D, HN-F or CCG issues a transaction request with a non-zero QoS QPC value
- The crosspoint incorrectly overrides the QPC value to zero

Implications

QoS functionality will be impaired due to the zero QPC value, cannot use RN-F pass-through QPC or any RN-I, RN-D, or CCG QoS regulator functionality. HN-F nodes do not have QoS regulators available for their requests.

Workarounds

Use the following workarounds if the QoS QPC value is corrupted:

- Configure to use the RN-F QoS regulators in the MXP instead of the pass-through value from the RN-F.
- Update HN-F QoS threshold logic to comprehend the zero values from RN-I, RN-D, and CCG.

3033427
CCG might not service IDE stop on the CXS interface

Status

Affects: CMN S3
Fault Type: Programmer Cat-B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

This affects IDE for CXL 2 type 3 host and device, SMP 64B IDE.

In a very rare scenario when IDE is enabled an IDE stop command is sent over CXS from the LLL controller.

Configurations affected

CMN configurations that enable CXL IDE

Conditions

This erratum occurs if the following conditions are met:

- Software quiesces traffic while IDE state is secure
- Protocol flits are no longer sent, which starts the protocol idle counter programmed in por_ccla_ull_idle_counter moving the IDE state from secure to protocol idle.
- The protocol idle counter overflows and a TMAC control flit is sent over CXS to the LLL. The IDE state stays in protocol idle state in this state until the truncation count in por_ccla_IDE_truncation_transmit_delay_control has been reached.
- The LLL sends an IDE stop command over CXS while in protocol idle state
- The IDE stop is ignored, and the IDE state goes back to secure mode after the truncation count has been exceeded

Implications

IDE might not be disabled so packing logic will continue to reserve space for MAC header, decreasing packing efficiency. The LLL controller/PHY may flag this as an error.

Workarounds

Use the following workarounds if a stop command is sent over CXS from the LLL controller.

1. Software quiesces traffic while IDE state is secure
2. Wait for por_ccla_IDE_outbound_state[0] = 0 then send IDE stop using write to por_ccla_cxl_ide_pyld [7:0] = 0x21

3043435
Snoop FIlter flush does not propagate Persistent CMO when FORCE_FLUSH_PCMO_EN is set

Status

Affects: CMN S3
Fault Type: Programmer Cat-B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Address-Based Flush (ABF), HN-F, or HN-S Power State transition to NOSFSLC state do not propagate Persistent CMO to downstream SN-F when the force PCMO configuration bit (hns_cfg_ctl.orce_flush_pcmo_en) is enabled.

Note that ABF is the expected flush mechanism for the Persist cachelines, Persist lines will be flushed before Power State transitions.

Configurations affected

Any CMN configuration with Persistent Memory.

Conditions

This erratum occurs when the FORCE_FLUSH_PCMO_EN feature is enabled (hns_cfg_ctl.force_flush_pcmo_en ==1'b1) and one of the following conditions are met:

- HN-F or HN-S transitions to the NOSFSLC power state that results in SF flush
- ABF sequence is triggered that results in SF flush

Implications

If the conditions are met, WriteBacks triggered by the SF flush will not propagate a PCMO to downstream SN-F.

Workarounds

Software must perform PCMOs to all cachelines in the address region vs. using ABF, no workaround required for the Power State transition flushes.

- DC CGDVADP
- DC CGDVAP

- DC CGVADP
- DC CGVAP
- DC CVADP
- DC CVAP

3085420
MPAM CSU Monitors might capture incorrect values

Status

Affects: CMN S3
Fault Type: Programmer Cat-B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

MPAM CSU monitoring functionality, including illegal PARTID or PMG checks, might result in incorrect results.

Configurations affected

All CMN configurations.

Conditions

This erratum occurs when MPAM CSU Monitoring is enabled.

Implications

If the condition is met, the following might occur:

- Incorrect MPAM INTREQ assertion and error logging for illegal PARTID or PMG or Monitor configurations for CSU monitor filtering, both false positive and false negative errors. The following INTREQ and registers are impacted:
- - **MPAM interrupt pins:** INTREQMPAMERR<NS/S/RT/RL>_NID*
  - **MPAM error status registers:** cmn_hns_<ns/s/rt/rl>_mpam_esr

- Incorrect CSU Monitor counts, which affects overall CSU Monitor functionality. The following registers are impacted:
  - cmn_hns_<ns/s/rt/rl>_msmon_csu
  - cmn_hns_<ns/s/rt/rl>_msmon_csu_capture
  - cmn_hns_<ns/s/rt/rl>_msmon_cfg_csu_flt

Workarounds

Software must ignore illegal PARTID/PMG INTREQ and error logging registers, and do not enable CSU Monitoring.

3189964
More than two XY route override can result in deadlocks

Status

Affects: CMN S3
Fault Type: Programmer Cat-B
Fault Status: Present in r0p0, r0p1. Fixed in r1p0

Description

Default XY routing can be overridden by programming up to 16 sourceID or targetID pairs in the por_mxp_xy_override_sel registers. The sourceID or targetID pairs in indexes 0 and 1 are the only indexes that result in XY overrides, indexes >1 are ignored.

Configurations affected

All CMN S3 configurations with the XY_OVERRIDE_CNT > 2.

Conditions

This occurs when the por_mxp_xy_override_sel registers with indexes > 1 are programmed with XY overrides.

Implications

If the conditions are met, either of the following will occur depending on if:

- The source or target pair is in an index > 1, the XY override behavior will not occur.
- Multiple MXPs require XY override programming and any MXP is in an index > 1, a deadlock will occur.

Workaround

Do not program por_mxp_xy_override_sel registers with indexes > 1, only 2 overrides are valid in CMN.

3223098
RN-I/RN-D can return same ARID reads out of order when AXI data interleaving is disabled

Status

Affects: CMN S3
Fault Type: Programmer Cat-B
Fault Status: Present in r0p0, r0p1. Fixed in r1p0

Description

A sequence of AXI reads with ARIDUNQS<port>, asserted and de-asserted can result in same ARID reads completing out of order, violating AXI protocol requirements, when the AXI port por_rn(i/d)_s<port>_port_control.s<port>dis_data_interleaving is enabled.

This only affects the port_control disable data interleaving and not the newer system disable data interlaving enabled via por_rn(i/d)_aux_ctl.sys_data_interleaving.

Configurations affected

All CMN configurations where AXI data interleaving is disabled for an RN-I or RN-D port.

Conditions

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

- port s<port>_dis_data_interleaving=1
- Mixed traffic with ARIDUNQS<port> asserted and de-asserted
- por_rn(i/d)_aux_ctl.dis_rreq_bypass=0 (default setting)

Implications

If the conditions are met, same ARID reads complete out of order, violating the AXI protocol.

Workaround

Set por_rn(i/d)_aux_ctl.dis_rreq_bypass=1, disabling the read request bypass.

Using this workaround adds 1 cycle of latency to the read request path because of the bypass path being disabled.

3245612
Incorrect SDC multi-cycle path constraints for 2xREQ configurations

Status

Affects: CMN S3
Fault Type: Programmer Cat-B
Fault Status: Present in r0p0, r0p1. Fixed in r1p0

Description

Incorrect Multi-cycle Path (MCP) constraints on device interfaces can result in deadlocks, the following SDC constraints are not valid:

```
set static_post_boot_state [filter_collection [all_registers] \
  "full_name =~ u_mxp_misc/rxlcrdrdy_q_reg_*"]
set_multicycle_path 2 -setup -from $static_post_boot_state
set_multicycle_path 1 -hold  -from $static_post_boot_state
```

Configurations affected

CMN configurations with 2xREQ enabled and the above MCPs applied in implementation.

Conditions

This erratum occurs when MCPs present in the SDC are used for implementation and timing closure.

Implications

If the condition is met, CMN device link interfaces may not activate, resulting in deadlocks.

Workaround

The workaround is to perform the reset/boot sequence at a slower frequency, half the target frequency. The rxlcrdrdy_q only performs flop transitions on reset de-assertion.

3363760
A continuous stream of DVM Operations requests by Peer DN or Remote chip requestors can starve Local DVM Syncs

Status

Affects: CMN S3
Fault Type: Programmer Cat-B
Fault Status: Present in r0p0, r0p1, r1p0. Fixed in r2p0

Description

In multi-DVM domain configurations, a DVM Node (DN) that receives a constant stream of DVM Operation (DVMOp) requests from a remote chip or Peer DN (PDN) requestors can result in local DVM Sync requests being starved.

Configurations affected

Configurations with multiple DVM domains.

Conditions

This erratum occurs if all the following conditions are met:

- DVM domains are configured to receive DVM requests from remote chips or PDNs.
- RN-Fs in the PDN's domain or remote chip send a continuous stream of DVMOps. For example, TLB Invalidate operations resulting a DN receiving a continuous stream of DVMOps from the PDN or remote chip(s) without DVM Syncs.
- The same DN receives DVM request from its local RN-Fs.

Implications

If the above conditions are met, the DVM Syncs sent from local RN-Fs might not complete, resulting in a deadlock.

Workaround

Configure CMN to a single DN domain using the boot-time software configuration. For details on DN domain configuration, see the Arm® Neoverse™ CMN S3(AE) Technical Reference Manual.

3606070
CCG CXL3.0 receiver does not support late poison

Status

Affects: CMN-S3
Fault Type: Programmer Cat-B
Fault Status: Present in r0p0, r0p1, r1p0. Fixed in r2p0.

Description

The CXL3.0 specification specifies support for late data poison. Late poison is in addition to the poison sent in Data messages. CMN ignores the late poison indication, and assertion can result in deadlock.

Configurations affected

CCG CXL3.0 configurations with the external controllers supporting CXL Late poison.

Conditions

This erratum occurs when a non-Arm CXL3.0 transmitter IP sends a late poison flit to the H slot of a standard flit 256B format or the HS slot of a latency optimized 128B format.

Implications

If the conditions are met, the receiver unpacking logic will ignore the late poison and use the empty data in the flit if there is rollover from the previous flit. The data in the flit sent after the late poison flit might be interpreted as a message, which can result in deadlocks.

Workaround

To prevent a deadlock, you must switch to the CXL2.0 protocol by programming the lower link layer PHY/controller to change the flit format from 256B to 68B when initializing the link.

Category B (rare)

2985283
Incorrect TagMatch response on partial writes with MTE Match

Status

Affects: CMN S3
Fault Type: Programmer Cat-B (Rare)
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Partial Write requests with MTE TagOp Match can cause an incorrect TagMatch response

Configurations affected

Any configuration with HN-F devices that use MTE without MTSX

Conditions

This erratum occurs when the following conditions are met:

- Non-Arm CPU issues non-allocating WriteUniquePtl with TagOp=Match and Tag=<partial>
- The System Level Cache has dirty data but without MTE Tag
- HN-F incorrectly responds with no TagMatch for the WriteUniquePtl

Implications

If the conditions are met, MTE Write Partial transactions that require TagMatch response can be incorrect. Partial write transactions might not respond with TagMatch.

Workarounds

Use the following workaround for the correct TagMatch response for partial write transactions, by setting cmn_hns_cfg_ctl.mte_no_sn_match to enable local match for non-Arm CPUs.

3066481
Dirty Memory Tag Extension tags can be dropped in On-Chip Memory mode

Status

Affects: CMN S3
Fault Type: Programmer Cat-B (Rare)
Fault Status: Present in r0p0. Fixed in r0p1.

Description

LDREX or STREX for cachelines in SD (SharedDirty) cache state can cause modified Memory Tag Extension (MTE) tags to be dropped when the cacheline is in On-Chip Memory (OCM).

Note that Arm CPUs do not support SD cache state.

Configurations affected

Any CMN S3 configuration with CPUs that implement SD cache state.

Conditions

This erratum occurs when all the following conditions are met:

- OCM mode is enabled, either all_way or address range based
- Non-Arm CPU issues LDREX or STREX for a cacheline address in SD state
- CMN is in NOSFSLC power state or the access hits an SF eviction

Implications

If the conditions are met, the modified MTE tag can be dropped resulting in MTE tag coherence issues.

Workarounds

Do not enable MTE in OCM mode.

Category C

2958415
System Level Cache cache lines in locked way can be evicted

Status

Affects: CMN S3
Fault Type: Programmer Cat-C
Fault Status: Present in r0p0, r0p1. Fixed in r1p0

Description

The System Level Cache (SLC) Way Locking feature allows cache lines to be allocated into specific ways of the cache based on address ranges. Any access to a locked cache line after allocation should hit the cache. There are conditions that can cause the locked cache lines to be evicted, causing subsequent accesses to miss the cache.

Configurations affected

Any configuration.

Conditions

This erratum occurs when all the following conditions are met:

- Locked region configured without enabling On-Chip Memory (OCM) mode
- Cache line in the locked address region allocates line to the SLC
- Non-allocating WriteUniqueFull or WriteUniqueZero transactions targeting SLC locked region hits the locked cache line

Implications

The locked line can be evicted if the conditions are met, resulting in a subsequent cache miss for a locked line. Allocating writes are required for SLC usage, so this issue should not impact the expected usage of locked regions. Note that this is primarily a performance and latency issue since the subsequent access will see memory latency instead of SLC hit latency. This behavior does not result in a functional issue.

Workaround

Use the following workarounds if the locked SLC cache lines are evicted:

1. When SLC locked region is enabled in non-OCM mode, set cmn_hns_cfg_ctl.wlu_alloc_on_hit to '1'b0'. This will force allocation for writes that hit the SLC irrespective of the allocation attribute.
2. Enable OCM mode for the locked region. Note this does not allow downstream memory accesses for the locked regions for SLC miss, so the initial allocation of data into the OCM region must be via writes instead of downstream memory reads.

2964003
Incorrect Correctable Error Logging in HN-S and HN-F components

Status

Affects: CMN S3
Fault Type: Programmer Cat-C
Fault Status: Present in r0p0, r0p1. Fixed in r1p0

Description

The Arm RAS 1.1 Architecture Spec requires the first Correctable Error (CE) increment the Correctable Error Repeat Counter (CECR) register. CMN S3 HN-S and HN-F incorrectly increment the Correctable Error Other Counter (CECO) register on the first CE.

Configurations affected

All CMN S3 configurations.

Conditions

HN-S or HN-F CE occurs due to a single-bit ECC correction in the Snoop Filter or System Level Cache RAMs.

Implications

HN-S or HN-F CECR and CECO counts may be off by 1 CE.

Workaround

When reading the CECR and CECO from registers which are non-zero, increment CECR by 1 and decrement CECO by 1.

2976084
Debug reads with simultaneous coherent traffic or dynamic power transitions can cause deadlock

Status

Affects: CMN S3
Fault Type: Programmer Cat-C
Fault Status: Present in r0p0, r0p1. Fixed in r1p0

Description

HN-F System Level Caches (SLC) and Snoop Filter (SF) Debug Reads with simultaneous coherent traffic or dynamic power retention transitions can cause a deadlock.

Configurations affected

Any configuration.

Conditions

This erratum occurs when the following conditions are met:

- Coherent transactions that require HN-F Snoop Filter allocation while performing SLC or SF debug read
- Dynamic retention mode is enabled while performing a SLC or SF debug read

Implications

A deadlock can occur if the conditions are met. Note that expected usage is performing the Debug Reads in the absence of traffic since traffic can change the state of the RAMs.

Workaround

Use the following workarounds to prevent a deadlock:

- Stop CPU (RN-F) and IO (RN-I) coherent traffic before issuing Debug Reads
- Disable Dynamic retention power transitions via cmn_hns_ppu_pwpr.dyn_en = 1'b0 (reset value)

3105737
Incorrect MPAM_MSMON_IDR value for NO_HW_OFLW_INTR bit [30]

Status

Affects: CMN S3
Fault Type: Programmer Cat-C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

CMN MPAM does not support the MPAM Monitor Overflow Interrupt feature, and the MPAM IDR capability register incorrectly indicates support of the feature.

Configurations affected

All configurations that use MPAM.

Conditions

Read the value of the MPAM_MSMON_IDR register and use the capability information.

Implications

The register will incorrectly indicate that hardware interrupts for overflow is supported.

Workaround

Software should not use the MPAM IDR capability register to determine support for the MPAM Monitor Overflow Interrupt features. Software may use CMN product and revision specific overrides for the NO_HW_OFLW_INTR capability.

3217599
HN-S Non-Secure, Root, or Realm RAS events may be reported in Secure error records

Status

Affects: CMN S3
Fault Type: Programmer Cat-C
Fault Status: Present in r0p0, r0p1. Fixed in r1p0

Description

Under specific micro-architectural conditions, SLC Data RAM Single-Bit Error (SBE) or Double-Bit Error (DBE) for Non-Secure (NS) accesses can update the Secure RAS error records.

Configurations affected

CMN configurations with SLC_TAG_LATENCY = 1.

Conditions

This occurs when there is a SLC Data RAM SBE or DBE on a NS/ Root/ Realm memory transaction.

Implications

If the conditions occur, Secure RAS error records may be updated for NS RAS events and a loss of RAS coverage for NS SBE and DBE errors.

In addtion, if the cmn_hns_errcapctl.secure_capture_control configuration bit is set to 1'b1, NS RAS error records may be updated for Root or Realm RAS events.

Workaround

No workaround available, must assume Secure RAS error records were updated by NS/Root/Realm RAS events, for example by checking the address to determine if it's in NS space.

3283582
On-Chip Memory Mode entrance and exit can result in data inconsistency

Status

Affects: CMN S3
Fault Type: Programmer Cat-C
Fault Status: Present in r0p0, r0p1. Fixed in r1p0

Description

The On-Chip Memory (OCM) entry and exit sequence documented in the Technical Reference Manual (TRM) might result in data inconsistency, a read after write might not return the correct data or prevent power state transitions after exit.

Configurations affected

All CMN S3 configurations.

Conditions

This erratum occurs when entering or exiting OCM mode following the TRM sequences.

Implications

If the condition is met, either of the following can occur:

- Data inconsistency in the OCM memory regions after entering OCM mode dynamically.
- Power state transitions do not complete after exiting OCM mode.

Workaround

You must enter OCM mode out of reset and exit via reset.

3355767
Incorrect MXP RAS ERRSRC logging information

Status

Affects: CMN S3
Fault Type: Programmer Cat-C
Fault Status: Present in r0p0, r0p1, r1p0. Fixed in r2p0

Description

The MXP ERRSRC field in the por_mxp_errmisc1 registers indicate the CHI channel and device port for MXP RAS events, and incorrect error sources are being logged for configurations with more than one MXP.

Configurations affected

All CMN configurations.

Conditions

This erratum occurs when your configuration reports either of the following errors:

- FLIT Parity
- Data Parity

Implications

If the conditions are met, the incorrect error source is logged in the por_mxp_errmisc1 ERRSRC register field, as shown in the following table.

	Expected ERRSRC	RTL Reported
RSP Port 0	'b00100	'b01000
RSP Port 1	'b00101	'b01001
RSP Port 2	'b00110	'b01010
RSP Port 3	'b00111	'b01011
SNP Port 0	'b01000	'b10000
SNP Port 1	'b01001	'b10001
SNP Port 2	'b01010	'b10010
SNP Port 3	'b01011	'b10011
DAT Port 0	'b01100	'b11000
DAT Port 1	'b01101	'b11001
DAT Port 2	'b01110	'b11010
DAT Port 3	'b01111	'b11011

Workaround

For FLIT Parity and Data Parity errors, use the table in the Implications section to determine the expected ERRSRC value.

3625665
HN-S RAS Overflow INTREQ not asserted on first Correctable Error after writing 0xFFFF to Correctable Error Counter

Status

Affects: CMN S3
Fault Type: Programmer Cat-C
Fault Status: Present in r0p0, r0p1, r1p0. Fixed in r2p0

Description

When the value of the Correctable Error Counter (CECR) is 0xFFFF, a Correctable Error (CE) of the same error type should result in an overflow event and RAS interrupt. This RAS event and interrupt does not occur if the CECR is written to 0xFFFF via configuration write.

Note that the expected use-case for writing 0xFFFF is software testing of the RAS handler. The RAS event INTREQ asserts correctly for all other values of CECR, or if the CECR naturally increments to 0xFFFF due to CEs.

Configurations affected

All CMN configurations.

Conditions

This occurs when both of the following conditions are met:

- A configuration write sets the CECR value to 0xFFFF.
- A CE occurs that reflects the same source in the ERRMISC1 register.

Implications

No RAS INTREQ will occur if the above conditions are met, which prevents usage of this sequence for software RAS handler testing.

Workaround

No workaround is required for normal operation. Write 0xFFFE to CECR and inject 2 CE to generate the RAS INTREQ for software test of the RAS handler.

Proprietary notice

(PRE-1121-V1.0)

Product and document information

Read the information in these sections to understand the release status of the product and documentation, and the conventions used in the Arm documents.

Product status

All products and Services provided by Arm require deliverables to be prepared and made available at different levels of completeness. The information in this document indicates the appropriate level of completeness for the associated deliverables.

Product completeness status

The information in this document is Final, that is for a developed product.

Product revision status

The rxpy identifier indicates the revision status of the product described in this manual, where:

rx

Identifies the major revision of the product.

py

Identifies the minor revision or modification status of the product.