Errata_FU540-C000_20210205

Proprietary Notice

Information in this document is provided “as is,” with all faults.

SiFive expressly disclaims all warranties, representations, and conditions of any kind, whether express or implied, including, but not limited to, the implied warranties or conditions of merchantability, fitness for a particular purpose and non-infringement.

SiFive does not assume any liability rising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation indirect, incidental, special, exemplary, or consequential damages.

SiFive reserves the right to make changes without further notice to any products herein.

Errata Classification

The document lists all of the known issues impacting the FU540 as of February 5, 2021.

The following table describes each errata category severity level (i.e. "CAT" level):

CAT-A	A **critical** error with **high probability** & the **absence of an effective workaround**.
CAT-B	A **significant** error with **high/medium probability** and an acceptable workaround, or a **minor error** with a **high** probability (regardless of workaround), or a **critical** error with **medium/low probability**.
CAT-C	A **minor** error with **high/medium probability** or **significant** error with **low probability** and an **acceptable workaround**.

The errata category classification is derived from the following impact/probability relationship:

Probability of an errata to manifest	Impact		
	Critical	Significant	Minor (feature limiting)
High	CAT-A	CAT-B	CAT-B
Medium	CAT-B	CAT-B	CAT-C
Low	CAT-B	CAT-C	CAT-C

CIP-234

Title

DMA can send out 1 extra read request to source memory

Implication

The DMA request sends 1 extra read request, but that read request is not written to the destination memory. Normally, this is benign (just produce extra traffic on the network). However, if the one extra request crosses the PMA boundary and accesses memory that is not available, the DMA will result in failure. There could also be issues if reading from memory regions with side effects.

Workaround

If DMA will end on a multiple of the transfer size, set up DMA transfer to 1 byte less than actually desired, leaving the last byte to software.

Impact

Medium

Probability

High

Category

CAT-B

CIP-253

Title

DRET does not raise illegal instruction when executed out of debug mode.

Implication

The RISC-V Debug Specifications states that `DRET` should result in an illegal instruction exception when executed outside of debug mode. When this erratum is present, in M-mode a `DRET` instruction does not cause an illegal instruction exception.

Workaround

None

Impact

Minor

Probability

Low

Category

CAT-C

CIP-257

Title

Opcodes `0b100xxxxxxxxxx00` do not raise illegal instruction exceptions as they ought to

Implication

Opcodes `0b100xxxxxxxxxx00` do not raise illegal instruction exceptions as they ought to. Instead, executing one of these opcodes will perform an atomic memory operation. The AMO is still properly permission-checked, so the unspecified behavior does not open a security hole.

Workaround

None.

Impact

Minor

Probability

Low

Category

CAT-C

CIP-286

Title

Debug Module/ROM Accessible in M-Mode

Implication

It is possible to access Debug Module memory region in M-Mode, whereas the Debug Specification indicates that region should only be accessible in Debug Mode.

Workaround

Do not access Debug Module memory region from M-Mode.

Impact

Minor

Probability

Low

Category

CAT-C

CIP-546

Title

When performance counters are set to count exceptions, they do not count other retirement events

Implication

It is not possible to use the same performance counter to count both exceptions and other retirement events (including instructions retired of specific type). Doing so will lead to incorrect counts for the other events.

Workaround

Use two separate counters: one for exception events and one for other instructions of interest.

Impact

Minor

Probability

Medium

Category

CAT-B

CIP-575

Title

L2 Sideband can report ECC error even after it was overwritten

Implication

The L2 Sideband includes a path to bypass data from older writes to newer hazardous requests, but still uses the corrected/uncorrected ECC result from the over-written entry for several cycles.

Workaround

Delay subsequent reads until the write has finished, such as by writing multiple times (3 times is sufficient).

Impact

Medium

Probability

Low

Category

CAT-C

CIP-576

Title

L2 response can report ECC error even after being overwritten

Implication

The L2 D-Channel response includes a path to bypass data from older writes to newer hazardous requests, but still uses the result of the ECC check (ie, ECC_correct/corrected_ECC_error/uncorrected_ECC_error) from the over-written entry for several cycles. This means that there is a short window of time during which an ECC error may be reported even once it has been overwritten.

Workaround

Tolerate multiple ECC errors reported for a single cache entry.

Impact

Minor

Probability

Low

Category

CAT-C

CIP-582

Title

L2 - Response can fail to report an ECC error if the data is read immediately after a corrupt write-back from the L1.

Implication

The L2 D-Channel response includes a path to bypass data from older writes to newer hazardous requests, but still uses the result of the ECC check (ie, ECC_correct/corrected_ECC_error/uncorrected_ECC_error) from the over-written entry for several cycles. This means that an ECC error may not cause a Bus Error Unit interrupt if an entry is read via a sub-cacheline sized read (eg a read from a core without an L1 DCache) within a few cycles of a cacheline write which is marked as corrupt.

For our designs, this situation will only be encountered when an L1 DCache line is evicted to the L2 Cache and an uncorrectable error is detected in that L1 line.

> **Note**
>
> In this scenario, the error will be detected during the eviction process. However, another core may read the data without the error being reported on that read.

Workaround

Detect all L1 ECC errors for all cores and use that as notification for uncorrectable errors.

Impact

Minor

Probability

Low

Category

CAT-C

CIP-589

Title

L2 Sideband can report no ECC error if read immediately after corrupt data is written

Implication

The L2 Sideband includes a path to bypass data from older writes to newer hazardous requests, but still uses the corrected/uncorrected ECC result from the over-written entry for several cycles.

Workaround

Delay subsequent reads until the write has finished, such as by writing multiple times (3 times is sufficient).

Impact

Medium

Probability

Low

Category

CAT-C

CIP-737

Title

mcause values does not reset to 0 after reset

Implication

`mcause` cannot be used to determine the cause of reset.

Workaround

Do not rely on the mcause value to determine reset condition; however, always assume that SiFive implementations do not distinguish different reset conditions.

Impact

Minor

Probability

High

Category

CAT-B

CIP-951

Title

Pseudo-Least-Recently-Used (PLRU) algorithm does not fully utilize non-power-of-2 cache ways or TLB Entries

Implication

Slight performance degradation — some ways of the cache or TLB will never be evicted.

Workaround

None needed, minor performance impact.

Impact

Minor

Probability

High

Category

CAT-B

CIP-1200

Title

Instruction TLB can fail to respect a non-global SFENCE

Implication

If an `SFENCE.VMA` with `rs1` != `x0` or `rs2` != `x0` happens on the same cycle as an I-TLB refill, the refill still occurs, even if the `SFENCE.VMA` should've flushed the entry being refilled.

This can lead to stale page mappings marked as valid in the TLB, which can in-turn allow unprivileged accesses, a security hole.

A global sfence.vma must be issued to properly invalidate TLB entries, which would have only performance implications and not functional.

Workaround

Flush the TLB using `SFENCE.VMA` `x0`, `x0`.

Impact

Critical

Probability

Low

Category

CAT-B

CIP-1464

Title

Chained triggers with both instruction and data never fire

Implication

Hardware allows 2 triggers to be chained, meaning both conditions must be satisfied at the same time for the trigger to fire. When a chain includes both instruction trigger and data address trigger, the breakpoint does not fire.

Workaround

Set a data trigger on any access to the data item, then in the GDB breakpoint command script, check whether the PC is the one you want and restart if not.

Impact

Minor

Probability

High

Category

CAT-B

FE-668

Title

ITIM de-allocation corrupts I-cache contents

Implication

When decreasing the amount of L1 I-cache memory mapped to the ITIM, instructions stored in the I-cache can become corrupted. Programs run on a core after ITIM memory has been decreased may exhibit unpredictable behavior.

Workaround

ITIM de-allocation can only be performed by the core that owns the ITIM using the following instruction sequence:

```
.align 3
sb x0, (t0)
fence.i
```

Impact

Medium

Probability

Medium

Category

CAT-B

FE-683

Title

Bus blocker may lock up bus on reconfiguration

Implication

Attempting to enable a bus blocker mid-transaction can cause the in-flight transaction to be blocked, resulting in system deadlock.

Workaround

Do not attempt to change BusBlocker settings once traffic is enabled through them. For example, if a bus blocker is used to disable access to DDR memory before the DDR interface is enabled, once the DDR interface is enabled, do not attempt to reconfigure the bus blocker.

Impact

Medium

Probability

Medium

Category

CAT-B

FE-866

Title
I2C interrupt can not be cleared

Implication
The I2C controller command `IACK` (interrupt acknowledge) does not work. The I2C controller's interrupt can not be lowered, rendering it unusable.

Workaround
Poll the I2C controller state to wait for TIP (transaction in progress) to go low.

Impact
Medium

Probability
High

Category
CAT-B

FE-1092

Title

Current DMI transaction doesn’t finish until JTAG TAP spends at least one cycle in Idle state.

Implication

If last scan through DR register performing DMI operation goes to JTAG Idle state and TCK clock immediately stops after entering idle then current transaction will not be completed until next TCK cycle.

Workaround

Let TCK run for at least one cycle in Idle state after each DMI transaction.

Impact

Minor

Probability

Low

Category

CAT-C

FE-1154

Title

CSRR instruction reads old value of fflags under certain circumstances

Implication

When a NaN is passed through `fadd` and the next instruction reads the `fcsr`, the NV bit is not set.

Workaround

Use the result of the floating-point instruction before reading the flags.

Impact

Medium

Probability

Low

Category

CAT-C

FE-1321

Title

Debug Transport Module - Transition through JTAG DR Capture state accepts DMI response even when sticky DMI busy bit is set.

Implication

Transition throgh JTAG DR Capture state accepts DMI response even when the DMI busy bit is set. This causes subsequent transaction to accept DMI response even after DMI Busy error, which, in turn, loses DMI Read data from previous transaction. It makes it difficult to recover from DMI Busy error in some cases.

Workaround

Put additional Idle `TCK` state cycles when implementing Debug protocol to avoid DMI busy bit getting set.

Impact

Medium

Probability

Medium

Category

CAT-B

FU-681

Title

High 24 address bits are ignored

Implication

When accessing memory, the high 24-bits of virtual and physical addresses are sometimes unchecked. This affects indirect jumps, returns, loads, stores, and atomics.

Workaround

Do not access out-of-bound addresses in software.

Impact

Medium

Probability

Low

Category

CAT-C

FU-740

Title

L2 ECC failed address reporting flawed

Implication

Under memory contention, an uncorrectable ECC failure in the L2 will sometimes report the wrong address in the registers `DatECCFailHigh` and `DatECCFailLow`. It is impossible to be certain what memory was corrupted when an uncorrectable L2 ECC failure occurs.

Workaround

Don’t rely on the address reported in software. Treat all L2 ECC uncorrectable failures as fatal.

Impact

Minor

Probability

Low

Category

CAT-C

FU-769

Title

The DPC CSR is not sign-extended

Implication

The DPC CSR correctly retains only the low 40 bits of the PC when entering debug mode. When the CSR is read, the result should be sign-extended to 64 bits but is not. The debugger reports the PC with the high 24 bits always zero. This does not affect return from debug mode (because the PC is also only 40 bits).

Workaround

The debugger can sign-extend DPC itself.

Impact

Medium

Probability

Medium

Category

CAT-B

FU-822

Title

E51 atomic operations not ordered correctly

Implication

Acquire/release ordering semantics on atomic operations in the E51 core do not work correctly. Loads and stores may appear to be re-ordered relative to atomic operations in a way that is illegal under the RISC-V memory model.

Workaround

Set both acquire and release bits on atomics run on the E51 core; e.g., use `amoor.d.aqrl` instead of `amoor.d.aq` or `amoor.d.rl`.

Impact

Medium

Probability

High

Category

CAT-B

FU-865

Title

Watchpoints fire after stores are issued

Implication

The RISC-V debug specification allows implementations to either break on the store instruction before it has been executed or to break on the instruction following a store after it has been executed. Cores with this errata break on the store, after it has been executed and self-report to the debugger that they do not execute watch-pointed stores, i.e., that `timing` is `before`.

Watchpoints on memory with side effects will cause that side effect to occur twice. For example, if a watchpoint is set on the UART TX register, a write to the UART TX register will cause a character to be transmitted and the watchpoint to fire. Once the program is resumed, that same character will be transmitted again. The same double-write will occur with watch-points on memory-backed addresses, but the second write typically has no visible effect.

Workaround

Do not put watchpoints on memory with side effects. Do not expect to see the old value in memory after a watchpoint has fired.

Impact

Medium

Probability

Medium

Category

CAT-B

FU-885

Title

Setting lock bit in NA4 and NAPOT does not allow writes to lower pmp reg

Implication

When PMP config registers are set to `NA4` or `NAPOT`, and the register has Lock bit set, they are no longer writeable. However, the register 'below' is also un-writeable.

> **Note**
>
> This is Correct operation for TOR addressing but not for Naturally Aligned (NA) addressing, locking 2 register instead of one in napot mode.

Workaround

Use other unlocked pmp registers.

Impact

Medium

Probability

High

Category

CAT-B

FU-1059

Title

A write to the L2 while flushing that cache line may be lost

Implication

The L2 can be flushed via control registers. If a write executes in the L2 pipeline following a flush to the same cache line, the write may be lost.

Workaround

In a single threaded context follow any L2 flush with a fence instruction. In a multi threaded context, synchronize the threads to avoid writing to a line being flushed.

Impact

Medium

Probability

Medium

Category

CAT-B

FU-1077

Title

PTW may cache stale translation that can propagate to the I/DTLB

Implication

On an `SFENCE.VMA` instruction, PTW internal caches are invalidated. However, in a short sequence of instructions, it is possible for the PTW to cache a stale transition and have it propagate to the I/DTLB:

1) An instruction which will modify the page tables is fetched.

2) An `SFENCE.VMA` instruction is fetched.

3) A speculative instruction fetch is performed and misses the ITLB, generating a PTW request for a translation which depends on the page table being modified.

4) The PTW request hits the PTE cache and skips a level of translation in the table walk.

5) The page tables are modified.

6) The `SFENCE.VMA` instruction invalidates the L2 TLB and PTE cache entries.

7) The PTW request continues, having used a stale intermediate translation from the PTE cache.

8) The PTW completes and fills the L2 TLB and PTE caches.

9) Later ITLB or DTLB misses can hit the PTW caches and be refilled with the stale translation.

Workaround

Instead of a single `SFENCE.VMA` instruction, execute `SFENCE.VMA x0, x0` twice.

Impact

Minor

Probability

Low

Category

CAT-C

FU-1089

Title

SFENCE with non-zero rs1 argument is broken when VM is disabled

Implication

`SFENCE` with `rs1` != `x0` is rarely, if ever, used when VM is disabled. If used, it does not flush the TLB line corresponding to the `rs1` argument in the presence of this bug.

Workaround

Use `rs1=x0` on SFENCE when VM is disabled

Impact

Medium

Probability

Low

Category

CAT-C

FU-1136

Title

ERESET_N assertion during certain SD card operations can cause subsequent boot to fail

Workaround

Either 1) never use `ERESET_N` (the FU540 "reset button") to reset the FU540, power-cycling the board instead; or 2) configure MSEL to load from a boot device other than SD.

Impact

Medium

Probability

Medium

Category

CAT-B

FU-1241

Title

pmpcfg register should not be set in R=0,W=1 condition

Implication

The above configuration can be set in the pmpcfg register and generates permission exceptions as such

Workaround

Adhere to the combination of the R and W permissions as per the RISC-V spec.

Impact

Minor

Probability

Low

Category

CAT-C

FU-1327

Title

Reversed polarity for `mcounteren` and `scounteren`

Implication

For the performance counters such as cycle or instret, zeroing either the `mcounteren` or the `scounteren` bit should disable the read access to these in user mode. Instead the design requires both enable registers to be cleared to do so.

Workaround

Reverse the polarity of the mcounteren and scounteren bits in software.

Impact

Medium

Probability

High

Category

CAT-B

FU-1329

Title

PMP does not properly compose with superpages

Implication

If either the PMP or PMAs are nonuniform across the entire superpage (1 GiB or 2 MiB), then the PMPs/PMAs will only be checked on the first 4 KiB subpage. In other words, the PMP/PMA check will act as though address bits 29:12 = 0 (for 1 GiB pages), or address bits 19:12 = 0 (for 2 MiB pages).

If PMPs and PMAs are both uniform across the entire superpage, then the PMPs and PMAs are checked correctly.

When 4 KiB pages are used, PMPs and PMAs are always checked correctly, regardless of PMP/PMA uniformity.

Workaround

1) To avoid granting S-mode permission to access memory that it should not be able to access, M-mode software should only grant access to a region with address bits 29:12 equal to zero if it also intends to grant access to the surrounding 1 GiB region. Using 1 GiB alignment for all PMPs is sufficient, but not necessary, to accomplish this.

2) To avoid unexpected access exceptions, S-mode software should use only 4 KiB pages to map regions that might not have uniform PMP/PMA settings.

Impact

Critical

Probability

Medium

Category

CAT-A

FU-1360

Title

Mask ROM code does not clear SPIFlash FCTRL register before accessing SDCard

Implication

For SPI controllers with built-in Memory-Mapped Flash capability, the `FCTRL` register is enabled by default to enable memory-mapped flash capability out of reset. Software must first clear the fctrl reg (SPI reg offset `0x60`) before attempting to use the controller in non-memory mapped mode. For example, in order to initializing and writing to/reading from an SD card.

The boot mode with ModeSelect = `0x8` is broken because the Mask ROM code assumes `spi.fctrl` = `0x0` during SD card initialization. SPI Controllers which are SPIFlash capable can't be used to access SDCard in the boot ROM.

Workaround

Design and use a Mask ROM boot method that does not attempt to access the SDCard via a SPIFlash capable SPI controller.

Impact

Critical

Probability

Medium

Category

CAT-B

FU-1461

Title

Debug hasreset feature not implemented

Implication

The RISC-V Debug specification describes a hasreset feature to determine when a hart being debugged has been reset. This is not implemented and always reports 0.

Workaround

Do not rely on the hasreset feature in debugger software.

Impact

Medium

Probability

High

Category

CAT-B