New issue

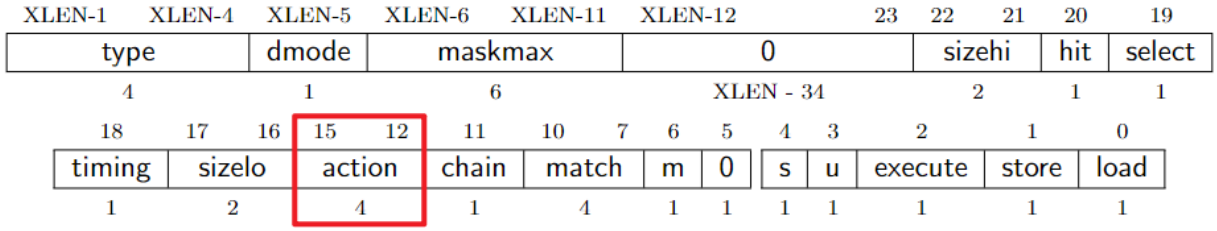
Jump to bottom

[Bug Report] Incorret mask for mcontrol.action #1032

Open **Phantom1003** opened this issue on Jun 16 · 2 comments

Phantom1003 commented on Jun 16 • edited Contributor

We found the mask for mcontrol.action is 0x3f, while this field is only 4 bits width.



riscv-isa-sim/riscv/triggers.cc
Line 44 in 89745ab

```
44      action = (triggers::action_t) get_field(val, MCONTROL_ACTION);
```

riscv-isa-sim/riscv/encoding.h
Line 102 in e6a2245

```
102     #define MCONTROL_ACTION     (0x3f<<12)
```

We triggered this bug by randomly writing data to csr.
If users try to set the sizelo field next to it (although it appears that spike does not yet support), it will cause an illegal action to be saved, and then the abort() will be triggered at line 337 below, causing the simulation to end.

riscv-isa-sim/riscv/execute.cc
Lines 327 to 337 in 89745ab

```
327     switch (t.action) {
328       case triggers::ACTION_DEBUG_MODE:
329         enter_debug_mode(DCSR_CAUSE_HWBP);
330         break;
331       case triggers::ACTION_DEBUG_EXCEPTION: {
332         trap_breakpoint trap(state.v, t.address);
333         take_trap(trap, pc);
```

```
334           break;
335         }
336         default:
337           abort();
```

> **@ProjectDimlight** helps reproduce the problem

cc to **@timsifive**

Phantom1003 commented on Jun 17 — Contributor, Author

Following is the test case we use, in this program we add a breakpoint to the 0x80000178 and specify the size field is 3.
This is possible because the manual specifies that the fields in mcontrol are WARL, so users may try to write the value they expected(0x200000000003005c), then we try to access 0x80000178, and the log shows that the emulation suddenly stops at 0x80000174.

```
core   0: 0x0000000080000140 (0x00000593) li      a1, 0
core   0: 0x0000000080000144 (0x7a059073) csrw    tselect, a1
core   0: 0x0000000080000148 (0x00000597) auipc   a1, 0x0
core   0: 0x000000008000014c (0x03058593) addi    a1, a1, 48
core   0: 0x0000000080000150 (0x7a259073) csrw    tdata2, a1
core   0: 0x0000000080000154 (0x7a2025f3) csrr    a1, tdata2
: reg 0 a1  ->  0x0000000080000178
core   0: 0x0000000080000158 (0x0010059b) addiw   a1, zero, 1
core   0: 0x000000008000015c (0x02d59593) slli    a1, a1, 45
core   0: 0x0000000080000160 (0x00358593) addi    a1, a1, 3
core   0: 0x0000000080000164 (0x01059593) slli    a1, a1, 16
core   0: 0x0000000080000168 (0x05c58593) addi    a1, a1, 92
core   0: 0x000000008000016c (0x7a159073) csrw    tdata1, a1
: reg 0 a1 -> 0x200000000003005c    (action was set to 48 here)
core   0: 0x0000000080000170 (0x7a1025f3) csrr    a1, tdata1
core   0: 0x0000000080000174 (0x00100193) li      gp, 1
[exit simulation]
```

spike-1.zip

timsifive commented on Jun 17 — Collaborator

This is definitely a bug, easily fixed by using the CSR_MCONTROL_ACTION macro instead of MCONTROL_ACTION (which is out-of-date) in triggers.cc. But I've got a bunch of other stuff going on and it will take a while before I get to this.

❤️ 1

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants