Detailed Findings

1 QEMU RISC-V

Analysis of the 2272 values lead to the following findings:

- **0b0000000000000000** is seen as valid instruction by the virtual machine but is defined as an illegal instruction in the RISC-V ISA specification.
- **0b100xxxxxxxxxxx00** and **0b100111xxx1xxxx01** are reserved within the RISC-V ISA specification but are both seen as valid instructions
- **C.ADDI16S, C.LUI** should be reserved if the nzimm field is zero, and **C.ADDI4SPN** when the nzuimm field is zero.
- **C.ANDI, C.SRLI64, C.SRAI64, C.SLLI64** instructions with immediate equal to zero are wrongfully marked as undocumented due to a disassembler fault. The latter three are legal HINT instructions when executed on a RV64 system.

The undocumented instructions in the reserved encoding spaces are executed as no-operations; these instructions and those related to C.ADDI16S, C.ADDI4SPN have no effect on processor state. The undocumented instructions related to C.LUI effectively sets the target register to zero. None of these undocumented instructions pose a reliability or security risk.

2 Hardware RISC-V

- **FENCE** instructions are wrongfully seen as illegal by the Capstone disassembler when the `rd` and `rs1` fields are not zero or the `fm` field is something other than `0b0000` or `0b1000`. The `rd` and `rs1` field along with the other possible values of the `fm` field are reserved for future extension. To ensure forward compatibility it is explicitly stated in the ISA specification that current implementations must treat any FENCE with values other then zero in these fields as a normal FENCE instruction.
- **FENCE.I** instructions are wrongfully seen as illegal by the Capstone disassembler when the `rd`, `rs1` or immediate fields are not zero. Same as the FENCE instruction.
- **FCVT.D.S, FCVT.D.W, FCVT.D.WU** instructions with a value in the rounding mode field other than 0 are wrongfully seen as illegal by the Capstone disassembler.
- **C.ANDI, C.SRLI64, C.SRAI64, C.SLLI64**: disassembler fault as in QEMU scan.