171 Instruction Break Point On VMRUN Instruction Leads To Unpredictable System Behavior

Description

VMRUN can be interrupted using a hardware instruction breakpoint using one of the debug registers, DR[0-3]. When the debug handler executes IRET, the processor is expected to execute the VMRUN instruction. However, in the failing case, the processor incorrectly re-enters the breakpoint handler with mixed guest and host state. This in turn causes erroneous execution and leads to unpredictable system behavior.

Potential Effect on System

Hypervisor developers will not be able to use hardware instruction break point on VMRUN instruction.

Suggested Workaround

Set the breakpoint on the instruction prior to VMRUN, then single step through VMRUN.

Fix Planned

No