738 Debug Exception Concurrent with Unintercepted SMI May Store Incorrect Stack Pointer in VMCB

Description

During processing of a RSM instruction to return from a system management interrupt (SMI) that occurred while in secure virtual machine (SVM) mode and without the SMI being intercepted, the processor core may not restore the guest stack pointer prior to presenting a debug exception (#DB) on the resumed guest instruction. In the event that this #DB is intercepted (or some other exception during the #DB processing is intercepted), the stack pointer from system management mode (SMM) may be saved into the virtual machine control block (VMCB offset 1D8h). There is no error if an interception does not occur during the #DB.

Potential Effect on System

Unpredictable program behavior when debug exceptions are enabled for a virtual machine, likely observed as a program or guest operating system crash. AMD has not observed this erratum with any commercially available software.

Suggested Workaround

None required.

Fix Planned

No