342 SMIs That Are Not Intercepted May Disable Interrupts

Description

During a resume from SMM that is due to an unintercepted SMI from a SVM guest context, the processor core does not restore the correct effective interrupt flag (IF) if the guest VMCB V_INTR_MASKING bit (offset 060h bit 24) is 1b. Under these conditions, the effective interrupt flag may be zero.

SMIs are not intercepted if VMCB offset 00Ch bit 2 is 0b or HWCR[SmmLock] (MSRC001_0015[0]) is 1b.

Potential Effect on System

The guest context may run with interrupts disabled until the next guest intercept. The hypervisor may not be able to regain control and the system may hang.

Suggested Workaround

Contact your AMD representative for information on a BIOS update.

Fix Planned

No