440 SMM Save State Host CR3 Value May Be Incorrect

Description

The processor writes bits 47:32 as 0000h of SMM Save State offset FF38h (Host CR3) when all of the following conditions are met:

- An SMI occurs while in a guest context.
- SMIs are not intercepted to the hypervisor and cause a direct transition from the guest to SMM mode.
- Nested paging is in use (VMCB offset 090h[0], NP_ENABLE, is 1b).
- The SVM Host CR3 address is greater than 4GB (VMCB Offset 0B0h, N_CR3, bits 47:32 are non-zero).
- Guest is not in long mode at the time of the SMI (guest Extended Feature Enable Register EFER[Long Mode Enable], MSRC000_0080[8], is 0b).

After the SMM BIOS executes an RSM instruction, the processor may then use this incorrect host CR3 for guest operation.

Potential Effect on System

Unpredictable system operation.

Suggested Workaround

Contact your AMD representative for information on a BIOS update.

Fix Planned

No