639 Processor May Have Incorrect Instruction Pointer Following a Specific CALL Instruction Encoding

Description

Under a highly specific and detailed set of internal timing conditions where the processor has performed at least 100 pushes, pops, near-calls and/or near-returns without executing any other operation that uses the stack pointer, the processor may incorrectly execute the following instruction:

- CALL RSP without any offset (instruction encoding FFD4h).

Under the above conditions, the processor does not execute the CALL instruction and instead may treat this instruction as if it is a NOP (no operation) instruction. The processor incorrectly updates the rIP to the address following the CALL.

This CALL RSP instruction should transfer instruction execution to the stack (i.e. it changes the rIP to the value that was in the rSP prior to the execution of the instruction). If the stack address is marked with a no-execute attribute (the NX bit is set in the page table), this generates a #GP exception. The stack is commonly marked with a no-execute attribute. As a result, the use of this instruction encoding is uncommon in applications.

Potential Effect on System

Unpredictable program behavior after incorrectly updating the instruction pointer (rIP). This behavior has not been observed with any commercially available software.

Suggested Workaround

Contact your AMD representative for information on a BIOS workaround.

Fix Planned

No