770 Processor Incorrectly Restores Guest Privilege Level after Unintercepted I/O C-state Request

Description

Following an unintercepted guest access to an I/O address that causes an entry to a C-state, the processor may enter core C6 (CC6) state and incorrectly clear the guest current privilege level (CPL) to zero.

Potential Effect on System

Unpredictable system behavior. AMD has not observed this erratum with any commercially available software.

Suggested Workaround

Hypervisors should intercept any guest accesses to the I/O registers associated with I/O C-states, to avoid the possibility that a guest operating system has allowed a non-privileged application to request I/O C-states.

To intercept these accesses, hypervisors should program the virtual machine control block (VMCB) I/O interception bits as follows:

- VMCB offset 00Ch bit 27 (IOIO_PROT) should be 1b.
- The I/O protection map should indicate interception on a read to the eight consecutive I/O addresses starting with the address specified at C-state Base Address Register[CstateAddr] (MSRC001_1073[15:0]). The physical address of the I/O protection map is at VMCB offset 040h.

Fix Planned

No