401 Software Interrupt Event Injection Ignores VMCB.NextRIP

Description

The processor does not use VMCB.NextRIP when event injection is used on an INTn, INT3, or INTO software interrupt. In the event that the injected instruction encounters a fault, the processor may incorrectly store the address following the software interrupt on the stack.

Potential Effect on System

Hypervisor software that uses event injection for software interrupts may cause an incorrect RIP to be saved to the stack. The software interrupt will not be injected after the fault is resolved.

Suggested Workaround

Hypervisor software should perform emulation of software interrupts, as if VMCB.NextRIP is not supported (CPUID Fn8000_000A_EDX[3]=0b).

Fix Planned

No