170 In SVM Mode Incorrect Code Bytes May Be Fetched After A World Switch

Description

On an exit from guest mode (world switch) when CR3 changes, under a highly specific and detailed set of conditions, incorrect code bytes may be forwarded from the prefetch buffer.

Potential Effect on System

Incorrect code bytes may be executed, resulting in unpredictable system behavior after world switches.

Suggested Workaround

Hypervisors should set TLB_CONTROL to Flush TLB on VMRUN in the VMCB.

Fix Planned

Yes