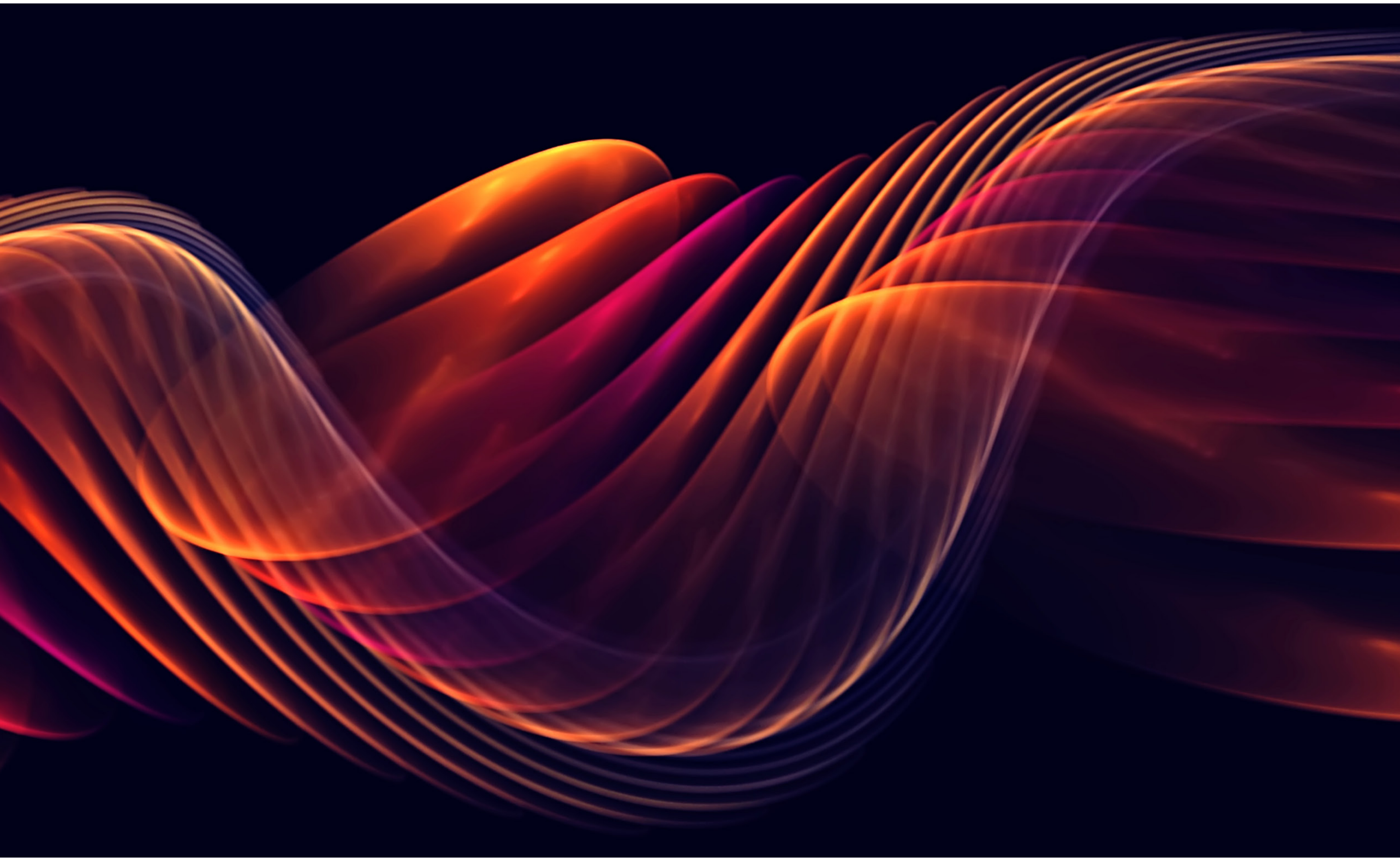

White Paper

TECHNICAL UPDATE REGARDING SPECULATIVE RETURN STACK OVERFLOW

REVISION 1.0 2023-08-08

1.INTRODUCTION

This document describes new architectural features and CPUID bits related to the Speculative Return Stack Overflow (SRSO) vulnerability. This information is intended to assist operating system and hypervisor developers with the mitigation of this vulnerability.

2. ENUMERATION OF NEW CAPABILITIES

AMD is defining three new CPUID bits to assist with the enumeration of capabilities related to SRSO:

CPUID Fn8000_0021_EAX[29] (SRSO_NO) – If this bit is 1, it indicates the CPU is not subject to the SRSO vulnerability.

CPUID Fn8000_0021_EAX[28] (IBPB_BRTYPE) – If this bit is 1, it indicates that MSR 49h (PRED_CMD) bit 0 (IBPB) flushes all branch type predictions from the CPU branch predictor.

CPUID Fn8000_0021_EAX[27] (SBPB) – If this bit is 1, it indicates support for the Selective Branch Predictor Barrier, discussed later.

3. BRANCH PREDICTOR BARRIER CHANGES

When IBPB_BRTYPE is supported, PRED_CMD bit 0 (IBPB) may be used to flush all older branch type predictions from the CPU branch predictor in addition to all older indirect branch predictions. On processors subject to the SRSO vulnerability, this may be used when transitioning between address spaces and/or privilege domains to mitigate SRSO by flushing any attacker-controlled branch type information. In some implementations, IBPB only flushes branch prediction information related to the current thread.

When SBPB is supported, software may write PRED_CMD bit 7 to 1 to initiate a Selective Branch Predictor Barrier (SBPB). This is a write-only bit. Setting this bit to 1 prevents the processor from using older indirect branch target predictions to influence future indirect branch predictions. This applies to JMP indirect, CALL indirect, and RET (return) instructions. SBPB is not guaranteed to flush older branch type predictions from the CPU branch predictor. In some implementations, SBPB only flushes indirect prediction information related to the current thread. If SRSO mitigation is not required or is disabled, software may use SBPB on context/virtual machine switch to help protect against vulnerabilities like Spectre v2.

If software writes PRED_CMD with both bits 0 and 7 set to 1, the processor performs an IBPB operation.

4. ENUMERATION ON EXISTING AMD CPUS

On AMD “Zen” and “Zen2” microarchitecture-based CPUs, the IBPB operation flushes branch type predictions from the branch predictor but does not set the IBPB_BRTYPE bit. Bare-metal software that detects a “Zen” or “Zen2” microarchitecture-based CPU should assume IBPB_BRTYPE=1 behavior exists. Hypervisor software should synthesize the value of IBPB_BRTYPE on these platforms so guest software can use CPUID to determine IBPB capabilities.

When the appropriate microcode patch is loaded on “Zen3” and “Zen4” microarchitecture-based CPUs, the IBPB operation flushes branch type predictions and the SBPB operation is supported but neither CPUID bit is set by hardware. Bare-metal software that detects a microcode patch version equal or greater than the version listed in AMD-SB-7005, the “Return Address Predictor Security Bulletin” *, should assume IBPB_BRTYPE=1 behavior and the existence of the SBPB feature. Hypervisor software should synthesize the value of both the IBPB_BRTYPE and SBPB CPUID bits on these platforms for use by guest software.

See https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7005.html for more information.

“Zen” microarchitecture-based CPUs include Family 17h Models 00-2Fh and Models 50-5Fh. “Zen2” microarchitecture-based CPUs include Family 17h Models 30-4Fh, Models 60-7Fh, and Models A0-AFh.
https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7005.html