

Zenbleed: AMD Zen 2 Vector Register Exploit Security Audit

Floating-Point RAT Speculative Zero-Optimization Vulnerabilities and Cross-VM Key Exfiltration Dynamics

EXECUTIVE ARCHITECTURAL SUMMARY: Zenbleed (CVE-2023-20593) represents one of the most severe speculative execution vulnerabilities ever discovered in modern x86 microprocessors. Affecting all AMD Zen 2 processors across consumer Ryzen, EPYC server, and mobile lines, Zenbleed enables unprivileged userspace processes to exfiltrate 256-bit AVX vector register states from any process, kernel thread, or virtual machine sharing the physical core at 30 kB/s with zero side-channel noise.

Microarchitectural Layer	Standard Non-Speculative Behavior	Speculative Misprediction State	Zenbleed Leakage Mechanic	Exfiltration Throughput
AVX YMM Register File	Physical 256-bit SRAM storage	Holds stale previous thread data	Un-cleared pointer exposed	30 kB / sec / core
Register Alias Table (RAT)	Updates pointer on instruction commit	Speculatively flips zero-bit (Z-bit)	Pointers out-of-sync with zero flag	Direct register read
vzeroupper Instruction	Zeroes upper 128-bit YMM lane	Mispredicted branch branch rollback	Rollback fails to re-allocate physical register	Zero-privilege leak
Virtual Machine Isolation	Hardware AMD-V guest boundary	Bypassed via SMT thread sharing	Cross-VM memory exfiltration	Full crypto-key theft

1. The Register Alias Table (RAT) & Zero-Optimization Shortcut

Modern out-of-order x86 processors decouple architectural registers (YMM0–YMM15) from physical register files (PRF) using a dynamic Register Alias Table (RAT). To accelerate AVX-to-SSE transition performance, AMD Zen 2 implemented an aggressive hardware optimization for the vzeroupper instruction.

- The Zero-Bit (Z-Bit) Shortcut: Rather than expending clock cycles and power writing actual zeros into physical SRAM register arrays, the Zen 2 RAT simply sets a metadata 'zero flag' on the register entry.
- Speculative Instruction Execution: If a vzeroupper instruction executes speculatively following a mispredicted branch, the RAT speculatively sets the Z-bit before branch resolution.

2. The Rollback Asymmetry Erratum: Exposing Stale Silicon State

When the branch predictor detects that the speculative branch was mispredicted, the processor flushes the Reorder Buffer (ROB) and rolls back the architectural state.

- The Critical Bug: Due to a logic flaw in the Zen 2 floating-point scheduler, the rollback mechanism restored the architectural register pointer but failed to synchronize the physical register allocation.
- Direct Plaintext Exposure: Downstream instructions reading the YMM register now read the raw, un-zeroed physical SRAM register file containing whatever data was left behind by previous threads.

3. Cross-VM Exfiltration Dynamics & Cryptographic Key Extraction

Because Simultaneous Multithreading (SMT) shares the physical floating-point register file between sibling logical threads on the same core, an unprivileged attacker can steal sensitive data across security boundaries:

- Hypervisor and VM Boundary Defeat: A tenant in a public cloud virtual machine can execute Zenbleed to capture vector memory operations performed by host processes or neighbor VMs.
- Memory String Function Theft: Highly optimized C runtime libraries (glibc) implement memcpy(), strcmp(), and strlen() using 256-bit AVX instructions. Passwords, TLS private keys, and encrypted payloads passing through libc are continuously scooped up into YMM registers.
- 30 kB/s Exfiltration Bandwidth: Zenbleed requires no cache timing or statistical inference; the attacker directly executes register-to-memory store instructions, pulling clean plaintext at wire speed.

4. Silicon Remediation vs. Software Mitigation Overheads

AMD resolved Zenbleed via microcode updates that set chicken-bit controls in Model-Specific Registers (MSR DE_CFG), forcing the processor to serialize vzeroupper execution. While microcode incurs minimal overhead on general compute, high-throughput AVX workloads suffer a 1% to 3% throughput penalty.

STRATEGIC ENGINEERING TAKEAWAYS & DEPLOYMENT RULES:

- Zenbleed directly exposes 256-bit AVX physical vector registers without relying on cache timing side channels.
- Unprivileged attackers can capture glibc memcpy() payloads across virtual machine boundaries at 30 kB/sec per core.
- Resolution requires microcode updates that serialize vector register clearing, incurring modest floating-point penalties.