Zenhammer: Rowhammer Fault Injection on AMD Zen 4/5 DDR5

Target Row Refresh Bypass, Non-Temporal Stores, and Kernel PTE Corruption

Author: Lesty Tech Systems Architecture Team | **Date:** November 5, 2026 | **Status:** Validated Engineering Reference | **Target:** Tier-1 Foundry, Silicon & Kernel Audits

EXECUTIVE ARCHITECTURAL ABSTRACT:

For years, DRAM manufacturers and system designers assumed that DDR5 memory, equipped with mandatory on-die Error Correction Codes (on-die ECC) and advanced Target Row Refresh (TRR) mitigations, was fundamentally immune to Rowhammer electromagnetic disturbance attacks. Furthermore, AMD Zen microarchitectures were historically considered difficult Rowhammer targets due to complex memory controller hashing. The Zenhammer research overturned both assumptions. By reverse-engineering AMD Zen memory interleaving functions and utilizing synchronized non-temporal streaming stores alongside precise cache flush sequences, Zenhammer triggers bit flips on commercial DDR5 chips, corrupting Linux kernel Page Table Entries (PTEs) for unprivileged root shell escalation.

1. Physical DRAM Disturbance & The DDR5 Scaled Cell Wall

As DRAM capacitor half-pitch shrunk below 14nm in 1α and 1β nodes, the storage capacitance per cell fell below 10 femtofarads. When a wordline is repeatedly toggled at high frequencies (ACTIVATE followed by PRECHARGE), rapid electromagnetic transients induce charge leakage across parasitic capacitance pathways to neighboring unselected capacitor storage nodes. While DDR5 introduced on-die SEC-DED (Single Error Correction, Double Error Detection) ECC to maintain manufacturing yields, on-die ECC operates strictly per 128-bit sub-channel word, leaving multi-bit disturbance patterns susceptible to silent bit flips.

2. Reverse-Engineering AMD Zen 3/4/5 Memory Interleaving Functions

Unlike Intel memory controllers that employ linear or published XOR hashing for bank address mapping, AMD Zen processors distribute physical addresses across channels, sub-channels, bank groups, and banks using undocumented proprietary linear feedback shift register (LFSR) functions. Zenhammer systematically recovered these hashing polynomials through high-resolution microbenchmarking, mapping arbitrary virtual pages into physical DRAM bank coordinates without administrative privileges.

Key Physical & Microarchitectural Benchmarks

Vulnerability Attribute	DDR4 (Intel/AMD)	DDR5 Intel (Blacksmith)	DDR5 AMD Zen 4 (Zenhammer)	Mitigated DDR5 (PRAC)
Hammer Activation Count	30,000 - 50,000	80,000 - 120,000	160,000 - 240,000	>1,000,000 (Safe)
TRR Bypass Pattern	Double-Sided Hammer	Frequency-based TRR Spoof	N-Sided Synchronized Pulse	Hardware Counter Clamp
On-Die ECC Resilience	No On-Die ECC	Single-Bit Flip Masked	Double-Bit Flipping in Word	Multi-Bit Lockout
Instruction Mechanism	CLFLUSH loop	CLFLUSHOPT loop	MOVNTDQ + SFENCE + Flush	Deterministic PRAC Refresh
Time to Privilege Escalation	15 - 90 seconds	45 - 180 seconds	90 - 300 seconds	Immune

3. Overcoming Target Row Refresh (TRR) via Many-Sided Activation

DRAM vendors embedded Target Row Refresh (TRR) logic inside DRAM dies to sample active row addresses and issue proactive refresh pulses to adjacent victim rows. However, TRR tracking state machines rely on finite internal sampling tables (typically 4 to 16 entries). Zenhammer executes complex 6-sided to 12-sided hammering patterns interspersed with dummy row activations. By flooding the TRR sampling logic, the victim rows are evicted from the internal tracking buffer before corrective refresh commands can be issued during refresh intervals (tREFI).

4. Non-Temporal Stores and Kernel PTE Exploitation

On AMD Zen architectures, the instruction clflushopt exhibits variable retirement latency when executing in tight loops. Zenhammer circumvents this by leveraging non-temporal streaming stores (movntdq / movnti), which bypass the L1/L2/L3 cache hierarchy entirely, writing directly to the write-combining buffer and memory bus. Once bit flips are reliably induced, attackers hammer memory pages allocated to Linux Page Table Entries (PTEs). Flipping a single bit in the physical page address frame or supervisor access bit immediately elevates an unprivileged process to root authority.

EXECUTIVE STRATEGIC TAKEAWAYS:

1. DDR5 on-die ECC is designed for manufacturing defect mitigation, not security; it fails against multi-bit Rowhammer disturbance patterns.

2. AMD Zen memory controllers are fully vulnerable once bank-selection XOR hashing functions are mapped via microbenchmarking.

3. Non-temporal streaming stores (MOVNT) provide an ultra-high-throughput alternative to cache flushes for bypassing Zen CPU caches.

4. Long-term hardware defense requires deterministic activation counting, such as Per-Row Activation Counting (PRAC), integrated into JEDEC standards.