

RowPress: DRAM Long-Row Activation Vulnerability Audit

Subthreshold Conduction, Gate Dielectric Stress, and Bypassing Target Row Refresh (TRR) with 100x Fewer Flips

EXECUTIVE ABSTRACT: RowPress (CVE-2023-44445) reveals a catastrophic hardware vulnerability in modern DDR4, DDR5, and LPDDR5 DRAM chips. Unlike Rowhammer which requires millions of rapid row precharges, RowPress keeps an aggressor row continuously activated for extended durations. Electrical charge leaks into victim cells via subthreshold conduction, inducing bit flips with up to 100x fewer activations and bypassing 100% of modern Target Row Refresh (TRR) mitigations.

DRAM Attack Vector	Physical Mechanism	Aggressor State	Min Activations for Flip	TRR Detection Status
Classic Rowhammer (2014)	Capacitive Crosstalk	Rapid Toggle (t_REFI)	150,000 - 300,000	Detected (High activation count)
Half-Double (2021)	Sub-array leakage	Many-row cascade	80,000 - 120,000	Partially Mitigated
RowPress (CVE-2023-44445)	Subthreshold Conduction	Continuous Open (t_agg > 10us)	1,200 - 4,500 (-98%)	UNDETECTED (Bypasses 100% of TRR)
RowHammer + RowPress	Combined stress	Hybrid pulsed open	600 - 1,500 (-99%)	UNDETECTED (Universal Bit Flips)

1. The Rowhammer Mitigations: Target Row Refresh (TRR)

Since the disclosure of Rowhammer in 2014, the DRAM industry has relied on **Target Row Refresh (TRR)**. DRAM chips contain internal hardware counters that track how many times a wordline is opened and closed within a refresh interval (t_REFI = 64 ms).

- Activation Counters: When an aggressor row exceeds an activation threshold (e.g., 30,000 pulses), TRR issues a preemptive refresh to neighboring victim rows, restoring lost capacitor charge before bits flip.
- The Flawed Assumption: All TRR algorithms assume that data disturbance requires *rapid, frequent, alternating activations*.

2. The RowPress Discovery: Long-Duration Wordline Stress

Researchers at ETH Zurich discovered that keeping a single DRAM wordline activated continuously causes charge leakage through an entirely different physical mechanism:

- Subthreshold Leakage: When a wordline voltage remains high (V_PP ≈ 2.5V - 3.0V), continuous electrostatic stress across the pass transistor gate induces subthreshold conduction in neighboring unselected cells.
- 100x Activation Reduction: By extending the row active time (t_agg) to several microseconds, bit flips occur with as few as 1,200 activations—two orders of magnitude below TRR detection thresholds!

3. Bypassing Modern DDR5 and LPDDR5 Hardware Defenses

Because RowPress operates well below the activation count trigger of on-die TRR engines, **100% of tested DDR4 and DDR5 modules from all major memory manufacturers are vulnerable**.

- Memory Controller Exploitation: An unprivileged attacker executes memory read instructions without `clflush`, keeping memory rows active in the memory controller's open-page policy.
- Privilege Escalation: RowPress flips bits in Linux kernel page tables (PTEs) and cryptographic keys in under 15 seconds without triggering a single TRR mitigation event.

4. Mitigation Realities: Bandwidth Destruction vs. Hardware Redesign

Software mitigations (such as enforcing aggressive closed-page policies or limiting maximum row active time in BIOS) collapse memory bandwidth by 30% to 50%. Complete remediation requires redesigning DRAM cell layouts and gate dielectrics in future DDR6 silicon.

STRATEGIC ARCHITECTURAL TAKEAWAYS

1. RowPress (CVE-2023-44445) induces DRAM bit flips by keeping wordlines open rather than pulsing them rapidly.
2. Requires up to 100x fewer row activations than Rowhammer, bypassing 100% of DDR4/DDR5 TRR hardware defenses.
3. Exploits subthreshold leakage; remediating via memory controller throttling incurs severe memory performance penalties.