

Downfall (Gather Data Sampling) Microarchitectural Security Audit

Transient Vector Execution Flaws and AVX-512 Performance Degradation in Cloud VMs

Published by **Lesty Tech Security Research Lab** | Date: October 20, 2026 | Reference: LESTY-ENG-2026-B6

1. The Speculative Architecture of SIMD Vector Gather

Modern high-performance x86-64 processors implement Advanced Vector Extensions (AVX2 and AVX-512) to accelerate floating-point matrix operations and cryptography. A critical component of these instruction sets is the vector gather primitive (e.g., `VGATHERDPD`, `VGATHERQPS`), which fetches non-contiguous memory locations into a single SIMD vector register. Because memory addresses are scattered arbitrarily across virtual space, the CPU executes vector gather using complex internal micro-coded state machines that interact speculatively with Line Fill Buffers (LFB) and the Vector Register File (VRF).

2. The Gather Data Sampling (GDS) Transient Leakage Mechanism

Security Disclosure (CVE-2022-40982): When an AVX gather instruction encounters a transient fault or page assist, the processor speculatively forward-propagates stale data remnants remaining inside internal execution registers (VRF) and fill buffers. An unprivileged attacker thread can execute malicious gather loops that speculatively absorb register contents from preceding processes, including OpenSSL AES keys, Linux /etc/shadow hashes, and browser encryption contexts across virtual machine boundaries.

3. Microcode Mitigation and Performance Fallout

Intel's hardware microcode mitigation (GDS_NO / MCU update) blocks transient vector forwarding by flushing internal gather buffers on context switches and serializing gather execution until page table checks complete. While this completely neutralizes data exfiltration, it introduces a severe computational penalty: scientific computing, AI inference, and ray-tracing workloads that rely heavily on AVX-512 gather suffer an immediate 15% to 39% performance regression.

ARCHITECTURAL BENCHMARK & PARAMETER TELEMETRY

Processor Architecture	Vulnerability Status	Leakage Rate (Unmitigated)	Microcode Mitigation	AVX-512 Performance Impact
Skylake / Cascade Lake	AFFECTED (CVE-2022-40982)	Up to 10 KB/sec	MCU Gather Flush	-22% to -38% in HPC
Ice Lake / Tiger Lake	AFFECTED (CVE-2022-40982)	Up to 12 KB/sec	MCU Gather Flush	-18% to -32% in Vector Math
Alder Lake / Raptor Lake	AFFECTED (CVE-2022-40982)	Up to 8 KB/sec	MCU Gather Flush	-14% to -26% in Blender/V-Ray
Sapphire Rapids / Emerald Rapids	HARDWARE FIXED	Not Vulnerable	Hardware Isolation	0% (Full Native Speed)

Zen 3 / Zen 4 / Zen 5	NOT VULNERABLE	Different Gather Engine	None Needed	0% (Immune)
-----------------------	----------------	-------------------------	-------------	-------------

© 2026 Lesty.tech Semiconductor & Systems Architecture Group. Released under Creative Commons Technical Attribution 4.0 International. For peer review inquiries and technical data verification, visit <https://lesty.tech>