TECHNICAL DOSSIER // MICROARCHITECTURAL SECURITY & CRYPTANALYSIS

Gather Data Sampling (GDS) Transient Leakage Analysis

Hardware Vector Register Fill Buffers, Cross-Thread Probing, and Architectural Mitigations

Published: October 30, 2026 | Distribution: Open Engineering Community | Document ID: LT-2026-B16-02

EXECUTIVE SUMMARY & MICROARCHITECTURAL SCOPE

Downfall (CVE-2022-40982), technically classified as Gather Data Sampling (GDS), is a severe hardware vulnerability affecting modern Intel processors with AVX2 and AVX-512 vector extensions. The flaw originates in how the internal memory execution engine handles vector gather instructions (vpgatherdd, vgatherqps), transiently exposing sensitive data resident in internal microarchitectural Register Fill Buffers (RFBs) across sibling hardware threads, virtual machines, and privilege boundaries.

Metric	Spectre-v2	Meltdown	MDS / ZombieLoad	Downfall (GDS)
Affected Engine	Branch Predictor	Out-of-Order Load	Line Fill Buffer (LFB)	Vector Gather RFB
Vector Support	Scalar x86	Scalar x86	Scalar / Vector Loads	AVX2 / AVX-512 Gather
Leakage Rate	~1-10 KB/s	~100 KB/s	~1-5 KB/s	Up to 10 KB/s
Cross-VM Leakage	Possible (BTB)	Host-Guest Bound	Yes (Sibling SMT)	Yes (Full SMT & SMR)
Mitigation Penalty	0.5% - 3% (IBRS)	2% - 8% (KPTI)	3% - 12% (MD_CLEAR)	15% - 42% (AVX/HPC)

1. Anatomy of Vector Gather Execution

Vector gather instructions load non-contiguous memory elements into a single SIMD register based on a vector of base offsets. To service multiple memory addresses simultaneously without stalling the out-of-order execution engine, Intel microarchitectures allocate internal Register Fill Buffers. During out-of-order speculative execution, if an address translation stalls or faults, the processor speculatively forwards stale data present in the transient fill buffer to dependent instructions.

2. Cross-Security Domain Transient Sampling

Because internal vector fill buffers are dynamically shared across simultaneous multi-threading (SMT) sibling logical cores and are not scrubbed on ring privilege transitions (Ring 3 to Ring 0) or VM-Exits, an unprivileged user process can repeatedly issue gather instructions to transiently sample high-value cryptographic secrets, including AES-NI keys, RSA exponents, and kernel memory pointers.

3. Intel Microcode Mitigation Mechanics

Intel released microcode updates that disable speculative gather forwarding by injecting hardware serialization barriers into the gather execution micro-op sequence. This effectively forces all internal fill buffers to be flushed and synchronized before dependent instructions can resolve, preventing speculative data forwarding from transient hardware buffers.

4. HPC Performance Impact and Mitigation Disabling

While typical server workloads experience a 1% to 3% slowdown, high-performance computing (HPC), financial modeling, and scientific simulations that rely heavily on sparse linear algebra and AVX-512 gather routines suffer catastrophic performance degradation between 15% and 42%. Cloud operators must evaluate whether to enforce microcode mitigations or disable SMT in isolated multi-tenant environments.

STRATEGIC ENGINEERING TAKEAWAYS & DEPLOYMENT CHECKLIST

- **Microarchitectural Target:** Internal Vector Register Fill Buffers (RFBs) shared across physical core SIMD execution units.
- **Exploit Primitive:** Speculative forwarding of unscrubbed line data during delayed address translation.
- **Microcode Serialization Hit:** Serialization stalls gather micro-op pipelines, incurring severe HPC performance penalties.
- **Kernel Toggling:** Linux kernel allows toggling via gather_data_sampling=off for dedicated non-shared compute clusters.