CacheWarp (CVE-2023-20592) Security Audit

Cache Coherence Exploitation, INVD Reversion, and Confidential VM Boundary Hijacking

Author: Lesty Tech Systems Architecture Team | **Date:** November 15, 2026 | **Status:** Validated Engineering Reference | **Target:** Tier-1 Foundry, Systems & Infrastructure Audits

EXECUTIVE ARCHITECTURAL ABSTRACT:

AMD Secure Encrypted Virtualization with Secure Nested Paging (SEV-SNP) provides cryptographic memory encryption and spatial integrity tracking to protect guest VMs from untrusted hypervisors. The CacheWarp exploit (CVE-2023-20592) bypasses these guarantees by exploiting a fundamental flaw in cache coherence invalidation. By executing unintercepted INVD instructions, a malicious hypervisor discards dirty cache lines sitting in CPU L1/L2 caches before write-back, reverting guest state to stale, pre-existing encrypted DRAM. This allows attackers to subvert sudo authentication, factor RSA-4096 private keys, and hijack confidential virtual machine control flow.

KEY PHYSICAL PARAMETERS & EXPERIMENTAL BENCHMARK TELEMETRY

Vulnerability Dimension	SEV (Zen 1)	SEV-ES (Zen 2)	SEV-SNP (Zen 3/4 Unpatched)	SEV-SNP (Patched / Zen 5)
Spatial Memory Integrity	No (Aliasing Possible)	No (Aliasing Possible)	Yes (Enforced by RMP)	Yes (Enforced by RMP)
Temporal Coherence Integrity	No Integrity	No Integrity	Vulnerable to INVD Reversion	Immune (INVD Trapped to WBINVD)
Authentication Subversion	Direct Memory Read	Direct Memory Read	CacheWarp Sudo/RSA Bypass	Protected against Reversion
Microcode Mitigation Tax	N/A	N/A	< 0.1% Throughput Penalty	0.0% Hardware Native

1. The Confidential Computing Trust Boundary

SEV-SNP assumes that malicious hypervisors cannot manipulate guest computation without tripping Reverse Map Table (RMP) or AES-XTS MAC integrity checks. However, RMP only enforces spatial ownership, blind to temporal desynchronization.

2. INVD Invalidation vs. Cryptographic Write-Back

Executing INVD discards dirty L1/L2 lines without writing back to DRAM. When the guest resumes, it loads valid but stale ciphertext previously written by itself, passing all hardware cryptographic integrity checks without errors.

TECHNICAL ANALYSIS CONTINUED: CACHEWARP (CVE-2023-20592) SECURITY AUDIT

3. Real-World Exploitation: Sudo & RSA-CRT Key Factorization

Reverting status variables turns authentication failures into root shells. In RSA-CRT signatures, reverting modular multiplication accumulators induces single-calculation faults, allowing instant factorization of private prime factors.

4. Official Microcode Remediation & Hardware Hardening

AMD microcode updates trap INVD instructions on Zen 3/Zen 4, automatically executing WBINVD write-back flushes. Next-generation SEV-TIO silicon incorporates hardware-enforced cryptographic write-back synchronizers across PCIe and memory.

STRATEGIC ENGINEERING TAKEAWAYS & DEPLOYMENT CHECKLIST:

- Temporal Coherence Risk: Proves that cryptographic memory encryption does not protect against temporal state reversion.
- RMP Integrity Blind Spot: Stale ciphertext originally generated by the guest passes all hardware MAC validation checks.
- Deterministic Fault Injection: Enables remote, software-only cryptographic fault injection without voltage or clock glitches.
- Microcode Trap Deployment: Host hypervisors must deploy AMD microcode updates trapping INVD to WBINVD with under 0.1% overhead.