

GhostWrite: T-Head RISC-V Hardware Vulnerability Architectural Dossier

Vector Instruction Pipeline MMU Bypasses, Direct Physical Memory Overwrites, and Silicon Errata Analysis

EXECUTIVE ARCHITECTURAL SUMMARY: GhostWrite (CVE-2024-44444) represents an unprecedented silicon security failure in the RISC-V ecosystem. Affecting the widely deployed T-Head XuanTie C910 and C920 processor cores, GhostWrite allows completely unprivileged userspace processes to directly read and write arbitrary physical memory addresses—completely bypassing the Memory Management Unit (MMU), virtual memory isolation, and page table access controls.

Security Boundary	Architectural Specification	GhostWrite Exploit Status	Attacker Capability	Hardware Remediation Feasibility
Virtual Memory (MMU)	Page Table Entry (PTE) access checks	Completely Bypassed (Zero check)	Direct physical RAM write	Impossible (Hardwired silicon erratum)
Supervisor / Kernel Mode	Privileged execution barrier (EL1/S-mode)	Bypassed from unprivileged EL0	Direct kernel code patch	Requires disabling Vector Unit
Process Isolation	Address space layout protection (ASLR)	Trivially defeated	Cross-process memory snooping	Software barrier ineffective
Vector Processing Unit	RISC-V Vector (RVV 0.7.1) ISA	Vulnerable execution pipeline	Payload delivery vector	Disabling RVV incurs 75% penalty

1. The Hardware Pipeline Erratum: Vector Store Address Translation Failure

Modern high-performance RISC-V processors implement out-of-order execution pipelines with hardware vector extensions. In the T-Head XuanTie C910 and C920 cores (powering millions of single-board computers, cloud nodes, and edge AI chips), a critical hardware design flaw exists inside the Vector Store execution unit.

- The Omission of PTE Validation: When executing specific vector store instructions (e.g., vsb.v, vsw.v), the hardware pipeline fails to issue a translation check against the Translation Lookaside Buffer (TLB) and Page Table Entries (PTE).
- Direct Physical Addressing: The vector execution pipeline treats the computed virtual address as an absolute physical bus address, transmitting write bursts directly onto the system AXI bus.

2. Exploitation Mechanics: Total System Takeover in 100 Milliseconds

Unlike speculative execution attacks (Spectre, Meltdown, PACMAN) that rely on subtle cache timing side-channels to *infer* data, GhostWrite is an architectural write primitive:

- Zero Speculation Required: The exploit executes architecturally, modifying physical memory permanently without rolling back.
- Overwriting Kernel Page Tables: An unprivileged process writes to physical memory addresses containing kernel page tables, setting its own UID to 0 (root) and modifying kernel code to disable SELinux/AppArmor.

3. Ecosystem Impact: Millions of RISC-V SoCs Compromised

The vulnerability affects massive commercial hardware deployments:

- Silicon Foundries Impacted: Alibaba T-Head XuanTie C910, Sophgo SG2042 (64-core server CPU), Milk-V Pioneer, BeagleV-Ahead, and Lichee Pi 4A.
- Cloud Multi-Tenancy Defeat: In containerized or virtualized cloud environments running on affected RISC-V chips, a single unprivileged container can write directly into neighboring tenant memory or hypervisor firmware.
- Permanent Silicon Flaw: Because the address validation logic is missing from the physical silicon RTL, no microcode update can fix the pipeline—the defect is physically etched in silicon.

4. The Devastating Remediation: Disabling the Vector Engine

The only effective mitigation available to operating system vendors (Linux, FreeBSD) is disabling the Vector Processing Unit entirely in the kernel. However, disabling vector acceleration crushes performance on AI, signal processing, and cryptography workloads by 50% to 80%.

STRATEGIC ENGINEERING TAKEAWAYS & DEPLOYMENT RULES:

- GhostWrite enables unprivileged processes to write directly to physical RAM, bypassing MMUs and page tables.
- Affects T-Head XuanTie C910/C920 cores powering major commercial RISC-V platforms and servers.
- Fixing the vulnerability without silicon respins requires completely disabling hardware vector units.