How Cloudflare addressed a cross-tenant data exposure vulnerability in Containers

PRIMARY

Publisher	Cloudflare
Published	2026-09-24
Retrieved	2026-09-28
Cite key	cloudflare2026how
URL	https://blog.cloudflare.com/containers-cross-tenant-vulnerability/

Assessment. The affected provider's own post-incident write-up. Primary for the timeline, the mechanism and the measured scope. Silent on individual customer notification and on whether personal data was implicated; both absences are used as absences, not as denials.

Claims drawn from this source. CLAIM-2026-09-28-01, CLAIM-2026-09-28-02, CLAIM-2026-09-28-03, CLAIM-2026-09-28-04, CLAIM-2026-09-28-05, CLAIM-2026-09-28-06, CLAIM-2026-09-28-07, CLAIM-2026-09-28-08, CLAIM-2026-09-28-09, CLAIM-2026-09-28-14

Published 24 September 2026.

Oren Yomtov of the Accomplish security research team reported the vulnerability on 4 September 2026 at 15:26 UTC through HackerOne.

Timeline. Sep 4, 15:26 UTC: report received. Sep 4, 18:45 UTC: Cloudflare confirmed the production flaw. Sep 4, 21:27 UTC: runtime fix merged. Sep 4, 23:15 UTC: rollout began. Sep 7, 06:13 UTC: rollout completed, cleanup started. Sep 19, 15:03 UTC: all pre-mitigation cached snapshots cleared.

Mechanism. The affected pools used Linux device mapper thin provisioning with skip_block_zeroing enabled, with 64 KiB block sizes. "When the thin volume backing a container's root disk was deleted, its physical blocks were returned to a pool that served workloads belonging to multiple customer accounts." When blocks were reassigned to new containers, "a smaller write changed only the written portion. The remainder could retain data from the block's previous owner." An attacker could write 4 KiB blocks into ext4 free-space regions, triggering allocation of previously used 64 KiB blocks. "A subsequent raw-device read could therefore observe bytes that the new container had never written."

Exposure. "The vulnerability would potentially have allowed for a customer with a Workers Paid account to recover residual data from storage blocks previously used by other customers' Containers."

Measured scope. "The researchers ultimately observed residual material on 18 of 24 placements and 20 of 22 underlying nodes across four continents", with 2,700 distinct foreign directory inodes identified through checksum analysis. The recovered blocks included "directory structures, database pages, and structurally complete SQLite databases." The researchers reported no third-party filenames or credentials were

disclosed to Cloudflare.

Cloudflare's position. "We saw no evidence that this specific attack vector was exploited by anyone else." "Cloudflare has patched this vulnerability and remediation does not require any further action by Cloudflare customers."

Products. The post names Cloudflare Sandboxes as built on Containers. Containers is a service available on the Workers Paid plan.

Not stated anywhere in the post: whether individual affected customers were notified; whether any CVE was assigned; whether personal data was implicated.