# Source dossier

## Nothing escaped — a container was handed a 64 KiB block with the last tenant's bytes still in it, and the duty that fires is documentation, not notification

Edition 2026-09-28 · narrative: Isolation you cannot audit is a claim, not a boundary — and the EU duty that fires is documentation, not notification · compiled 2026-09-28

## Claims index

| Claim | Statement | Status | Sources |
|---|---|---|---|
| CLAIM-2026-09-28-01 | Cloudflare published its account of a cross-tenant data exposure vulnerability in Cloudflare Containers on 24 September 2026. | verified | cloudflare2026how |
| CLAIM-2026-09-28-02 | Oren Yomtov of the Accomplish security research team reported the vulnerability through HackerOne on 4 September 2026 at 15:26 UTC; Cloudflare confirmed the production flaw at 18:45 UTC and merged a runtime fix at 21:27 UTC the same day. | verified | cloudflare2026how |
| CLAIM-2026-09-28-03 | Rollout of the runtime fix began 4 September 2026 at 23:15 UTC and completed 7 September 2026 at 06:13 UTC; all pre-mitigation cached snapshots were cleared by 19 September 2026 at 15:03 UTC. | verified | cloudflare2026how |
| CLAIM-2026-09-28-04 | The affected storage pools used Linux device mapper thin provisioning with skip_block_zeroing enabled and 64 KiB block sizes; when a block was reassigned to a new container, a smaller write changed only the written portion and the remainder could retain data from the block's previous owner. | verified | cloudflare2026how |
| CLAIM-2026-09-28-05 | The vulnerability would potentially have allowed a customer with a Workers Paid account to recover residual data from storage blocks previously used by other customers' Containers; a 4 KiB write into ext4 free space triggered allocation of a previously used block and a subsequent raw-device read could observe bytes the new container had never written. | verified | cloudflare2026how |
| CLAIM-2026-09-28-06 | The researchers observed residual material on 18 of 24 placements and 20 of 22 underlying nodes across four continents, and identified 2,700 distinct foreign directory inodes through checksum analysis. | verified | cloudflare2026how, bleepingcom2026cloudflar |
| CLAIM-2026-09-28-07 | The recovered blocks included directory structures, database pages and structurally complete SQLite databases. | verified | cloudflare2026how |

| Claim | Statement | Status | Sources |
|---|---|---|---|
| CLAIM-2026-09-28-08 | Cloudflare stated it saw no evidence that this specific attack vector was exploited by anyone else, and that remediation does not require any further action by Cloudflare customers. | verified | cloudflare2026how |
| CLAIM-2026-09-28-09 | Cloudflare's post names Cloudflare Sandboxes as built on Cloudflare Containers, a service available on the Workers Paid plan. | verified | cloudflare2026how |
| CLAIM-2026-09-28-10 | GDPR Article 33(5) requires the controller to document any personal data breaches, comprising the facts relating to the breach, its effects and the remedial action taken, and provides that the documentation shall enable the supervisory authority to verify compliance with Article 33. | verified | intersoftco2026article |
| CLAIM-2026-09-28-11 | GDPR Article 33(1) requires notification to the supervisory authority without undue delay and where feasible not later than 72 hours after the controller becomes aware, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons; Article 33(2) requires the processor to notify the controller without undue delay after becoming aware. | verified | intersoftco2026article |
| CLAIM-2026-09-28-12 | GDPR Article 28(3)(f) requires the processor to assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36, taking into account the nature of processing and the information available to the processor; Article 28(3)(h) requires the processor to make available all information necessary to demonstrate compliance and to allow for and contribute to audits. | verified | intersoftco2026processor |
| CLAIM-2026-09-28-13 | GDPR Article 28(1) requires the controller to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures. | verified | intersoftco2026processor |
| CLAIM-2026-09-28-14 | Neither Cloudflare's 24 September 2026 post nor BleepingComputer's 27 September 2026 coverage states that individual affected customers were notified, and neither states that a CVE identifier was assigned. | verified | cloudflare2026how, bleepingcom2026cloudflar |

Only claims marked **verified** may carry a post. **single-source** may appear as hedged context; **disputed** must not be published at all.

# 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.

# Cloudflare fixes Containers cross-tenant flaw exposing customer data

**SECONDARY**

| | |
|---|---|
| **Publisher** | BleepingComputer |
| **Published** | 2026-09-27 |
| **Retrieved** | 2026-09-28 |
| **Cite key** | bleepingcom2026cloudflar |
| **URL** | https://www.bleepingcomputer.com/news/security/cloudflare-fixes-containers-cross-tenant-flaw-exposing-customer-data/ |

**Assessment.** Independent trade-press write-up, used only to corroborate the researcher attribution and the 18-of-24 / 20-of-22 figures. Carries no figure the provider's own post does not. Publication date 27 September is a coverage date, not the event date: the disclosure is Cloudflare's, dated 24 September.

**Claims drawn from this source.** CLAIM-2026-09-28-06, CLAIM-2026-09-28-14

Published 27 September 2026.

Attributes the finding to Oren Yomtov of the technology company Accomplish.

Quotes Cloudflare: "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."

Figures: 18 of 24 container placements tested contained residual data; 20 of 22 underlying nodes tested showed recoverable data.

Describes Containers as a service available on the Workers Paid plan, running alongside Cloudflare Workers. Does not name other Cloudflare products built on Containers.

Does not state whether Cloudflare notified affected customers. No bug bounty amount stated. No CVE stated.

# Article 33 GDPR — Notification of a personal data breach to the supervisory authority

**PRIMARY**

| | |
|---|---|
| **Publisher** | Intersoft Consulting |
| **Published** | 2026-01-01 |
| **Retrieved** | 2026-09-28 |
| **Cite key** | intersoftco2026article |
| **URL** | https://gdpr-info.eu/art-33-gdpr/ |

**Assessment.** Regulation text. Paragraph 5 is the operative provision for this edition and is quoted in full.

**Claims drawn from this source.** CLAIM-2026-09-28-10, CLAIM-2026-09-28-11

Article 33(1). "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

Article 33(2). "The processor shall notify the controller without undue delay after becoming aware of a personal data breach."

Article 33(3). The notification shall at least (a) describe the nature of the breach including where possible the categories and approximate number of data subjects and of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point; (c) describe the likely consequences; (d) describe the measures taken or proposed.

Article 33(4). "Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay."

Article 33(5). "The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."

# Processor — Article 28 GDPR

**PRIMARY**

| | |
|---|---|
| **Publisher** | Intersoft Consulting |
| **Published** | 2026-01-01 |
| **Retrieved** | 2026-09-28 |
| **Cite key** | intersoftco2026processor |
| **URL** | https://gdpr-info.eu/art-28-gdpr/ |

**Assessment.** Regulation text. (3)(f) and (3)(h) are the contractual levers named in the edition; (3)(f)'s closing qualifier bounds the assistance to information the processor holds.

**Claims drawn from this source.** CLAIM-2026-09-28-12, CLAIM-2026-09-28-13

Article 28(1). "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

Article 28(3) chapeau. Processing by a processor shall be governed by a contract or other legal act binding on the processor with regard to the controller. That contract shall stipulate in particular that the processor:

(c) takes all measures required pursuant to Article 32;

(f) "assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor";

(h) "makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller."