All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
2 days
to the Build It Summit CFP

VOL. I · NO. 302 THURSDAY, OCTOBER 29, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ KERNEL
CISA gives agencies until October 31 to patch the kernel flaw behind 25 rooted firewalls P.2

◆ CI/CD
The GitLab Onigmo flaw is now exploited, and Alpine rebuilt its own server P.2

◆ DATA PLATFORMS
Airbnb cuts embedding staleness from two days to under a minute with Chronon P.2

STREAMING SECURITY

An unset JWKS URL lets anyone forge a Kafka superuser token

Apache Kafka disclosed 12 CVEs on October 28, fixed in 4.2.2, 4.3.2 and 4.4.0. The JWT bypass needs a setting, not an upgrade.

COMPILED FROM APACHE KAFKA CVE LIST, OCTOBER 28; DAILY CYBERSECURITY, OCTOBER 29

Kafka 4.1.0 to 4.3.0 brokers using SASL/OAUTHBEARER without sasl.oauthbearer.jwks.endpoint.url skip JWT signature checks (CVE-2026-110985). Set the URL; fixed versions refuse to start without it. Also set expected issuer and audience (CVE-2026-110952).

Five flaws exhaust memory: a batch of about 90 bytes can allocate 2 GiB, so also bound max.decompressed.message.bytes. A principal with no grants can read broker files and environment variables, and Kafka Connect leaks resolved secrets.

No exploitation is reported. Daily CyberSecurity says six are rated Important; Kafka's page gives no ratings. Strimzi 1.3.0 already offers Kafka 4.2.2.

Full story → kafka.apache.org/community/cve-list securityonline.info/apache-kafka-vulnerabilities-jwt-bypass

KAFKA'S 12 CVES, BY KIND

5	MEMORY EXHAUSTION
3	AUTHENTICATION
2	SECRET OR FILE EXPOSURE
2	CRASH OR HANG

Grouped from the descriptions on Kafka's CVE page, October 28, 2026.

OPEN MODELS

Nemotron 3.5 Transcribe leads open speech models with 4B active parameters

Released October 28 with Granary v2, 463,062 hours of speech in 48 languages. The benchmarks are NVIDIA's; the post names no licence.

COMPILED FROM HUGGING FACE BLOG (NVIDIA), OCTOBER 28

The open-weight hybrid Mamba-Transformer mixture of experts, about 30B parameters with 4B active, transcribes, attributes speakers, translates and answers questions about audio. Prompts steer it, for example with medical spellings.

NVIDIA reports 5.33% average WER on the Open ASR English board, first among open-weight models, and 4.62% across seven languages. A forthcoming NVFP4 build transcribes 100 hours in under three minutes on one RTX PRO 6000.

It serves on vLLM and SGLang-Omni, and is built for recordings, not live streams.

Full story → huggingface.co/blog/nvidia/nemotron-transcribe-granary

KUBERNETES

Kubernetes 1.37.2 arrives late, and DRA taints now evict

Four patch releases on October 28, 15 days after target.

COMPILED FROM KUBERNETES CHANGELOGS ON GITHUB, OCTOBER 28

1.36.6, 1.35.10 and 1.34.13 came too, all on Go 1.26.10. NoExecute DeviceTaintRules now evict pods using DRA-backed extended resources. No CVEs; next round November 10.

Full story → github.com/kubernetes/kubernetes/blob/master/CHANGELOG/CHANGELOG-1.37.md

AI GATEWAYS

LiteLLM Enterprise proxies leak their master key, at 10.0

GHSA-w4c7-34wj-hqm8, October 28. Unlicensed installs are safe.

COMPILED FROM DAILY CYBERSECURITY, OCTOBER 28

One unauthenticated request exfiltrates LITELLM_MASTER_KEY and provider keys. Take 1.103.10, 1.104.8, 1.105.6 or 1.106.5 and rotate keys.

Full story → securityonline.info/litellm-vulnerability-master-key-leak

MLOPS

MLflow's file-read flaw was probed within a day

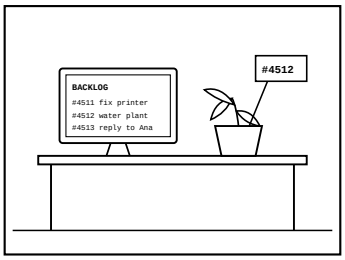
MLflow 3.17.0 fixes it and a 9.8 RCE.

COMPILED FROM DAILY CYBERSECURITY, OCTOBER 28

Previdian's honeypots saw CVE-2026-116690 tried after its October 27 CVE record. Upgrade and enable authentication.

Full story → securityonline.info/mlflow-vulnerability-exploited-poc

CARTOON OF THE DAY



Drawing: Claude

It escalated itself to P1 this morning.

WHY IT'S FUNNY The wilting office plant has planted a sign in its own pot with a ticket number, the same item that sits untouched in its owner's backlog. Plants usually suffer in silence; this one has worked out that only work with a ticket number gets done.

DATES TO WATCH
Events and calls for papers

Oct 29–30 EVENT
Dutch Cloud Native Day, Utrecht

Oct 30 EVENT
Kubernetes Community Days Budapest

Oct 31 CFP
Build It Summit (Paris, Dec 1): talks due

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

Core-provider 2.13.41 stops calling an unknown health reason healthy

October 29, 2026 — Nine components shipped on October 28 and 29, including installer 0.3.467, provider-runtime 1.7.0 and the first audit release.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

core-provider 2.13.38–2.13.41 · Oct 28–29
- Health reason splits converging from unhealthy.

github.com/krateo-platformops/core-provider/releases

installer 0.3.464–0.3.467 · Oct 28
- Pins core-provider 2.13.40; adds audit-worm.

github.com/krateo-platformops/installer/releases

provider-runtime 1.5.3–1.7.0 · Oct 28
- Names an unresolved create; needs Go 1.26.

github.com/krateo-platformops/provider-runtime/releases

snowplow 1.12.57 · Oct 28
- RESTAction writes sent once, never on failure.

github.com/krateo-platformops/snowplow/releases

frontend 1.8.13–1.8.14 · Oct 28
- Event streams reconnect after drops.

github.com/krateo-platformops/frontend/releases

portal 1.8.85 · Oct 28
- RBAC scoping fixed for composition lists.

github.com/krateo-platformops/portal/releases

oasgen-provider 0.37.0–0.39.0 · Oct 28
- OpenAPI validation keywords reach CRDs.

github.com/krateo-platformops/oasgen-provider/releases

observability 3.1.25–3.1.27 · Oct 28
- Tamper-evidence chart for the audit trail.

github.com/krateo-platformops/observability/releases

audit 0.1.0 · Oct 28
- First release: an AuditEvent emitter.

github.com/krateo-platformops/audit/releases

Latest elsewhere: sse-proxy 1.2.0 (Oct 27), alert-provider 0.2.53 (Oct 23), git-provider 0.15.6 (Sep 28).

KRATEO AGENTIKO

Merged into main this week

Krateo Agentiko notifications could not be read this morning.

NEWS IN BRIEF

KERNEL

CISA gives agencies until October 31 to patch the kernel flaw behind 25 rooted firewalls

CVE-2026-46300 (7.8), called Fragnesia, entered KEV on October 28. Dream researchers found it chained with PHP2Shell to root 24 perimeter firewalls and a management server from October 23. Fixed kernels include 6.1.174, 6.6.141, 6.12.91 and 6.18.33.

— Daily CyberSecurity, October 28 and 29
securityonline.info/cisa-kev-linux-kernel-php2shell-vmware-esx
securityonline.info/php2shell-exploit-fragnesia-roots-firewalls

CI/CD

The GitLab Onigmo flaw is now exploited, and Alpine rebuilt its own server

Crafted CI configs hit Alpine's unpatched GitLab on October 20 and 21 with CVE-2026-97229 (10.0). Alpine found no proof of success, but reset all passwords and keys, and says packages were not touched. Take GitLab 19.2.8, 19.3.5 or 19.4.2, and Ruby 3.3.13, 3.4.12 or 4.0.9 for custom builds.

— Daily CyberSecurity, October 28
securityonline.info/alpine-linux-gitlab-cve-2026-97229

JAVA

A public reproducer bypasses jackson-databind's type checks, at 9.8

CVE-2026-110879 hides blocked classes inside generic type arguments or arrays; with Spring present, the demo starts a process. Fixed in 2.18.12, 2.21.8, 2.22.4, 3.1.8 and 3.2.4. Not seen exploited.

— Daily CyberSecurity, October 29
securityonline.info/jackson-databind-vulnerability-cve-2026-110879-poc

CI/CD

Jenkins 2.588 fixes 15 flaws, including a setup-wizard race to admin

The October 28 advisory rates 13 High, several leading to code execution on the controller; many need only Overall/Read. Upgrade to 2.588 or LTS 2.580.2.

— Daily CyberSecurity, October 28
securityonline.info/jenkins-vulnerabilities-october-2026

DATA PLATFORMS

Airbnb cuts embedding staleness from two days to under a minute with Chronon

Push Mode and an in-stream model transform update embeddings 10 to 30 seconds after guest activity. Offline NDCG rose 1.67% and uncancelled bookings about 0.33%. Both features are in open-source Chronon.

— InfoQ, October 28
www.infoq.com/news/2026/10/airbnb-chronon-recommendation

AI RESEARCH

Anthropic says an internal model found a zero-click Linux RCE over multipath TCP

CVE-2026-98432 is patched in all stable branches; Google has fixed 62 Chrome CVEs from the same work. The report is Anthropic's own, and the exploit details are not independently verified.

— Daily CyberSecurity, October 28
securityonline.info/claude-ai-vulnerability-research

EDGE

Cloudflare's KV Instant reads at 1.62 ms p99, for at most 1 MB per namespace

Quicksilver, its internal config store, opens as a private beta: writes reach 300 locations in 256 ms at p99, against 4.38 s for classic KV. Storage costs $100 per MB a month.

— InfoQ, October 28
www.infoq.com/news/2026/10/workers-kv-instant

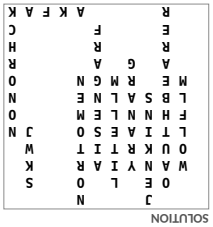
PUZZLE · WORD SEARCH

Ten words from today's two pages are hidden in the grid.

FIND CHRONON · FRAGNESIA · GRANARY · JENKINS · JWKS · KAFKA · LITELLM · MLFLOW · NEMOTRON · OAUTHBEARER

Y	F	P	J	Y	G	F	N	F	D	L	T
S	Y	O	E	B	L	M	O	I	B	S	Y
U	W	A	N	Y	I	A	R	A	F	K	U
B	O	U	K	R	T	I	T	C	B	W	A
Y	L	T	I	A	E	S	O	I	F	J	N
O	F	H	N	N	L	E	M	L	B	N	O
G	L	B	S	A	L	N	E	T	C	V	N
D	M	E	W	R	M	G	N	G	A	P	O
B	G	A	P	G	D	A	I	W	A	C	R
E	Y	R	B	R	M	R	O	V	O	V	H
U	T	E	U	E	D	F	V	D	I	L	C
V	D	R	U	V	Y	F	A	K	F	A	K

Words run in every direction, also backwards.



SOLUTION