All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
8 days
to the Build It Summit CFP

VOL. I · NO. 296 FRIDAY, OCTOBER 23, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ TRUST STORES
The eMudhra distrust now ships in Istio, Crossplane, Argo CD and Prometheus P.2

◆ CONTAINERS
Two 9.4 flaws let a standard Portainer user take over the Docker host P.2

◆ MESSAGING
Pulsar fixes 13 flaws, and the retired Pulsar Manager gets no patch at 10.0 P.2

SUPPLY CHAIN

LiteLLM 1.107.0 shipped a credential stealer to PyPI and four image tags

Built from a lookalike repository one hyphen off the real one, it was live for about 101 minutes on October 21. Pin 1.106.2.

COMPILED FROM SOCKET AND WIZ RESEARCH, OCTOBER 21-22; DAILY CYBERSECURITY

The release workflow pulled source from Berri-AI/litellm, not BerriAI/litellm; the tagged source lacks the hidden "cook" folder. Startup hooks run the payload whenever Python starts, even if LiteLLM is never imported.

It takes cloud, Kubernetes and Vault credentials, SSH keys, AI tool logins and the proxy's provider keys. Wiz counts about 49,000 downloads and saw stolen AWS roles tested against Bedrock 4.5 hours later.

Block 1.107.0 and the tags v1.107.0, latest, main-latest and main-stable. Isolate hosts, rotate secrets from a clean machine, pin digests.

Full story → socket.dev/blog/litellm-compromise www.wiz.io/blog/litellm-compromised-steals-credentials securityonline.info/litellm-supply-chain-attack

LITELLM 1.107.0 IN FOUR NUMBERS

101 MINUTES LIVE ON PYPI
49 DOWNLOADS, THOUSANDS
16 STEALER MODULES
7 MINUTES TO SOCKET'S ALERT

Published 11:39 UTC, quarantined 13:20 UTC (Wiz). Downloads from ClickPy, via Wiz. No attribution yet.

AGENTIC AI

Open Responses and Agent Skills join the Agentic AI Foundation

Four projects arrived October 22 at AGNTCon + MCPCon in San Jose, taking the Linux Foundation body to 10, from three at its launch.

COMPILED FROM LINUX FOUNDATION AND AAIF PRESS RELEASE, OCTOBER 22

OpenAI gives Open Responses, a specification for multi--provider LLM interfaces based on its Responses API: a shared schema, consistent streaming events and extensible tooling. Anthropic gives Agent Skills, a format for instructions, scripts and resources that agents load on demand.

Hugging Face gives OpenEnv, reinforcement learning environments delivered as containerised services that speak MCP and the Gym protocol. Alibaba gives OpenSandbox, with unified sandbox APIs and Docker and Kubernetes runtimes.

The announcement gives no licences or adoption figures. OpenSandbox is the piece that runs on a cluster.

Full story → www.linuxfoundation.org/press/agentic-ai-foundation-announces-four-new-projects-agent-skills-open-responses-openenv-and-opensandbox aaif.io/news/agentic-ai-foundation-announces-four-new-projects

PLATFORM SECURITY

Railway says decrypted variables were taken

Detected October 21; builds paused in all regions.

COMPILED FROM DAILY CYBERSECURITY, OCTOBER 22

Railway thinks the attacker wanted AI keys. Rotate every variable, reset database credentials, redeploy when builds return.

Full story → securityonline.info/railway-security-incident

BATCH SCHEDULING

Kueue 0.20.3 stops early quota release

Released October 22, with 0.19.10.

COMPILED FROM KUEUE RELEASES ON GITHUB

A StatefulSet scaled to zero freed quota while Pods still ran. 0.19.10 also fixes a TrainJob never admitted.

Full story → github.com/kubernetes-sigs/kueue/releases/tag/v0.20.3

LINUX KERNEL

ZDI made ksmbd flaws public

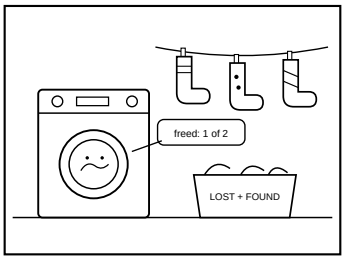
Two 9.0 bugs, unpatched, no CVE IDs.

COMPILED FROM DAILY CYBERSECURITY, OCTOBER 23

Posted to LKML on October 22. Disable ksmbd if unused; block port 445.

Full story → securityonline.info/linux-kernel-vulnerabilities-ksmbd-zdi-public

CARTOON OF THE DAY



Drawing: Claude

Garbage collection finished. One sock per pair reclaimed.

WHY IT'S FUNNY The washing machine is drawn as a very proud garbage collector that reports how much it freed. Every cycle it 'reclaims' exactly one sock of each pair, so the line fills with odd socks and the basket with orphans. Nobody has ever found where the freed socks go.

DATES TO WATCH

Events and calls for papers

Oct 24 EVENT
Kubernetes Community Days Nigeria (Lagos) and Indonesia (Bandung)

Oct 27 EVENT
Cloud Native Days Norway, Bergen

Oct 28 ONLINE
Cloud Native Live: AI inference with Crossplane

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

Portal splits into per-page charts; collectors redact JWTs

October 23, 2026 — Portal 1.8.78 to 1.8.84 and installer 0.3.443 moved ten pages into their own charts with breaking value changes; alerts can now fire on metrics.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

portal 1.8.84 · Oct 22

- Breaking: per-page charts; readerGroups defaults removed; devs reach five pages.

github.com/krateo-platformops/portal/releases

installer 0.3.449 · Oct 22

- 0.3.443 breaking: dataNamespace removed; 65 components, up from 55.

github.com/krateo-platformops/installer/releases

snowplow 1.12.53 · Oct 22

- Go 1.26.10 and x/net 0.60.0; 1.12.52 cache readiness fixes.

github.com/krateo-platformops/snowplow/releases

observability 3.1.22 · Oct 22

- Collectors redact JWTs by attribute value.

github.com/krateo-platformops/observability/releases

alert-provider 0.2.52 · Oct 22

- Metric CR: alerts can fire on a metric.

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

Latest elsewhere: frontend 1.8.10 (Oct 22), core-provider 2.13.26 (Oct 19), oasgen-provider 0.32.0 (Oct 19).

KRATEO AGENTIKO

Merged into main this week

Krateo Agentiko notifications could not be read this morning.

NEWS IN BRIEF

TRUST STORES

The eMudhra distrust now ships in Istio, Crossplane, Argo CD and Prometheus

Istio 1.31.3, Crossplane 2.4.3, Argo CD 3.3.18 and Prometheus 3.15.1, out October 21-22, move to Go 1.26.10 or newer and drop the roots from their images. Istio tracks it as CVE-2026-111943.

— Istio, Crossplane, Argo CD and Prometheus release notes

istio.io/latest/news/releases/1.31.x/announcing-1.31.3

github.com/crossplane/crossplane/releases

CONTAINERS

Two 9.4 flaws let a standard Portainer user take over the Docker host

Both let a non-admin bind-mount host files and reach root; one extends a bypass that survived two earlier fixes. Upgrade to 2.45.2. Reported October 22.

— Daily CyberSecurity

securityonline.info/portainer-vulnerabilities-bind-mount-bypass

MESSAGING

Pulsar fixes 13 flaws, and the retired Pulsar Manager gets no patch at 10.0

Disclosed October 21: brokers need 4.0.14 or 4.2.5; CVE-2026-105869 (9.2) trusts roles from unverified tokens. Remove Pulsar Manager (CVE-2026-105944) and rotate token signing keys.

— Daily CyberSecurity, October 22

securityonline.info/apache-pulsar-vulnerabilities-iotdb-patched

OBSERVABILITY

An OpenTelemetry Collector pipeline cuts a coding agent's metrics from 300 series to 12

A CNCF member post from Bindplane by Dynatrace, October 22: on Collector contrib 0.161.0, dropping session attributes keeps totals within half a percent, and log and trace bytes halve without sampling.

— CNCF blog

www.cncf.io/blog/2026/10/22/filtering-and-reducing-ai-agent-telemetry-with-the-opentelemetry-collector

NETWORKING

Cilium 1.20 moves to Gateway API 1.6 and lets plugins into the datapath

Released September 14, covered by InfoQ October 21: TCPRoute, UDPRoute, ListenerSets and ExternalAuth. bpf.datapathMode=auto picks netkit on Linux 6.8+; veth stays the default.

— InfoQ

www.infoq.com/news/2026/10/cilium-120-kubernetes-networking

AI AGENTS

Harbor runs each agent eval task in its own Docker microVM

InfoQ, October 22: each task gets a Docker Sandbox with its own kernel, and Cloud Sandboxes can cut internet access after setup. Docker tested 64 concurrent tasks.

— InfoQ

www.infoq.com/news/2026/10/ai-agents-harbor-docker

IDENTITY

Netflix swaps a Spark job's AWS role for a short-lived internal certificate

InfoQ, October 21: the Spark driver attests once with a pre-signed STS request, checked against signed control-plane metadata, then passes credentials to executors.

— InfoQ

www.infoq.com/news/2026/10/netflix-workload-attestation-aws

ENGINEERING DATA

Agents raised resolved work 12%, while review time rose 49%

A study of 700+ firms on data from vendor Jellyfish: agents lifted lines of code 30% but resolved issues 12%. InfoQ, October 22; authors not named.

— InfoQ

www.infoq.com/news/2026/10/jellyfish-ai-productivity

KUBECTL TIP

`kubectl cordon foo`

Stop new Pods before a kernel patch *(kubernetes.io)*

KUBECTL TIP

`kubectl scale --replicas=3 rs/foo`

Scale a ReplicaSet to three *(kubernetes.io)*

PUZZLE · WORD SEARCH

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

FIND CILIUM · ISTIO · KSMBD · KUEUE · LITELLM · NETFLIX · PORTAINER · PULSAR · RAILWAY · SANDBOX

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

Words run in every direction, also backwards.



SOLUTION