All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
1 day
to the OSC Kolkata CFP

VOL. I · NO. 308 WEDNESDAY, NOVEMBER 4, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ DEVELOPER PORTALS
Backstage 1.56.3 adds Zensical as Material for MkDocs shuts down P.2

◆ LLM APIS
Claude Message Threads keep conversation history on the server P.2

◆ FINOPS
AWS says 2027 capacity is largely sold out, with On-Demand held back P.2

AI SUPPLY CHAIN

Booby-trapped models on Hugging Face mine crypto on self-hosted GPU servers

Pluto Research found 31 malicious repositories on Hugging Face and ModelScope, aimed at Xinference and GPUStack hosts. The code runs on import; no malicious weights are needed.

COMPILED FROM DAILY CYBERSECURITY, NOVEMBER 3, ON RESEARCH BY PLUTO RESEARCH

Each repository ships a 42-byte safetensors file and custom modelling code that runs when a loader sets trust_remote_code=True. With 13 linked models they drew more than 32,000 downloads; Pluto says that "measures downloads, not confirmed infections or unique victims."

The payload installs the peakminer cryptominer, a watchdog, reverse shells and a container-escape script. There is no CVE.

What to do: look for /tmp/.cch/ on GPU hosts, require authentication on Xinference APIs, restrict egress from ML clusters, pin model revisions and review code before enabling trust_remote_code.

Full story → securityonline.info/hugging-face-malware-gpu-mining pluto.security/blog/hugging-face-malware-campaign-load-mine

THE CAMPAIGN, SEP-OCT

31	MALICIOUS MODEL REPOS
32	DOWNLOADS, THOUSANDS
13	LINKED MODELS
7	UPLOADER ACCOUNTS

Pluto Research via Daily CyberSecurity, November 3. Downloads are not confirmed infections.

AI ON KUBERNETES

OpenKruise Agents 0.6 doubles its CRDs to 12 to police agent sandboxes

The November 3 release adds L4 traffic policies, L7 security profiles and credential injection, from 283 merged pull requests since 0.3.0.

COMPILED FROM CNCF BLOG, NOVEMBER 3

Two new components, traffic-control-plane and traffic-proxy, take the count from four to six. New CRDs include PoolAutoscaler, TrafficPolicy and SecurityProfile. Credentials are injected from Kubernetes Secrets, so keys stay outside the sandbox.

A CheckpointRestore update mode keeps the root filesystem, and PoolAutoscaler scales on watermarks and cron. In-place resize of a running pod needs Kubernetes 1.33 or newer.

Caveat: a maintainer wrote the post, and its gateway figures are "theoretical upper bounds, not committed service metrics."

Full story → www.cncf.io/blog/2026/11/03/openkruise-agents-v0-6-0-leaping-ahead-in-agent-sandbox-security-and-automation

KUBERNETES SECURITY

Standalone Fleet needs 0.16.3 to close a 9.4 path to cluster-admin

It came with last week's Rancher fixes, but also hits Fleet run alone.

COMPILED FROM GITHUB ADVISORIES, OCTOBER 29; DAILY CYBERSECURITY, NOVEMBER 4

CVE-2026-94290 lets a user with workspace rights become cluster-admin on Rancher's local cluster; GitHub rates it 9.4, Daily CyberSecurity 9.1. Fleet 0.16.3, 0.15.8, 0.14.12 and 0.13.17 fix it.

Full story → github.com/rancher/fleet/security/advisories/GHSA-qfmw-gw96-ffcr securityonline.info/rancher-fleet-vulnerabilities-cve-2026-94290

CONFIGURATION MANAGEMENT

OpenVox and Puppet servers face a 9.4 RCE with a public proof of concept

With autosign on, the chain needs no credentials.

COMPILED FROM OPENVOX ADVISORY, NOVEMBER 3; DAILY CYBERSECURITY, NOVEMBER 4

Code runs as the puppet user, with "access to the CA signing key". Fixed in OpenVox Server 9.2.0 and 8.18.0, Agent 9.3.0 and 8.32.0, and Puppet Enterprise 2026.0.1 and older-line updates; open source Puppet gets none.

Full story → github.com/OpenVoxProject/openvox/security/advisories/GHSA-ffr6-rwpm-p5wq securityonline.info/puppet-server-rce-cve-2026-115731-poc

OBSERVABILITY

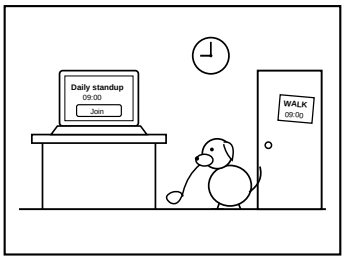
LinkedIn traces app taps end to end

COMPILED FROM INFOQ, NOVEMBER 3

A pageForestId groups a screen's request traces, Kafka carries the spans and ClickHouse keeps them.

Continued on page 2

CARTOON OF THE DAY



Drawing: Claude

Two daily standups at nine. Only one attendee will reschedule.

WHY IT'S FUNNY The laptop announces the team's nine o'clock standup, while the dog sits by the door with its leash and its own note: walk at nine. The dog's daily meeting is older, shorter and, unlike the video call, never gets moved.

DATES TO WATCH
Events and calls for papers

Nov 5 CFP
Open Source Conference Kolkata (Dec 5): talks due

Nov 8 EVENT
CNCF Maintainer Summit, Salt Lake City

Nov 9 EVENT
Platform Engineering Day, ArgoCon, BackstageCon and FluxCon NA, Salt Lake City

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

core-provider closes a redirect credential leak

November 4, 2026 — Nineteen releases on November 3 and 4: core-provider stops credentials following cross-host redirects and authn survives key rotation.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

core-provider 2.13.55 · Nov 3
- No credentials on cross-host redirects.

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

authn 0.32.0–0.33.0 · Nov 3
- Tokens survive signing-key rotation.

github.com/krateo-platformops/authn/releases

oasgen-provider 0.50.0 · Nov 3
- Host allowlist for credentialed calls.

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

alert-provider 0.2.58–0.2.59 · Nov 3
- Ratio alerts and an idle-window guard.

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

portal, frontend, observability 1.8.88, 1.8.19, 3.1.34 · Nov 3-4
- Service-desk queue; SLO span metrics.

github.com/krateo-platformops/portal/releases

installer 0.3.490–0.3.496 · Nov 3-4
- Pins authn 0.32.0 and core-provider 2.13.54.

github.com/krateo-platformops/installer/releases

Latest elsewhere: snowplow 1.12.64 (Nov 1), sse-proxy 1.3.0 (Nov 1), provider-runtime 1.7.2 (Oct 31), helm-render-service 0.5.0 (Sep 30).

KRATEO AGENTIKO

Merged into main this week

Krateo Agentiko notifications could not be read this morning.

CONTINUED FROM PAGE 1 · OBSERVABILITY

LinkedIn OTel

Full story → www.infoq.com/news/2026/11/linkedin-opentelemetry-journey

NEWS IN BRIEF

DEVELOPER PORTALS

Backstage 1.56.3 adds Zensical as Material for MkDocs shuts down

The November 2 patch adds an experimental Zensical engine for TechDocs. Its notes say Material for MkDocs shuts down on November 5.

— GitHub, backstage/backstage v1.56.3, November 2
github.com/backstage/backstage/releases/tag/v1.56.3

MONITORING

Prometheus 3.16 nears with query cost estimates and integral()

The November 3 candidate puts both behind feature flags. With TLS in --web.config.file, the default external URL becomes https.

— GitHub, prometheus/prometheus v3.16.0-rc.4, November 3
github.com/prometheus/prometheus/releases/tag/v3.16.0-rc.4

NETWORKING

Cilium 1.21 previews BPF masquerading by default and unnumbered BGP

The November 2 pre-release adds mTLS validation on Gateway API frontends and deprecates the XDP prefilter.

— GitHub, cilium/cilium v1.21.0-pre.4, November 2
github.com/cilium/cilium/releases/tag/v1.21.0-pre.4

AI INFERENCE

SGLang 0.5.23 runs MoE models larger than GPU memory on one consumer card

Paged Experts is opt-in in the November 2 release, which also runs on TPU7x and adds Muse Spark Open.

— GitHub, sgl-project/sglang v0.5.23, November 2
github.com/sgl-project/sglang/releases/tag/v0.5.23

LLM APIS

Claude Message Threads keep conversation history on the server

Clients send only the new prompt and the last message ID. A secondary report gives payloads down from 800 KB to 1.8 KB, prices unchanged; threads expire after five idle minutes.

— Daily CyberSecurity, November 3
securityonline.info/claude-message-threads-api

FINOPS

AWS says 2027 capacity is largely sold out, with On-Demand held back

Andy Jassy said on October 23 that "a good chunk of 2028 is sold out"; David Linthicum says reports overstate it. Consider capacity reservations.

— InfoQ, November 1
www.infoq.com/news/2026/11/aws-capacity-sold-out

LOCAL LLMS

Ollama 0.40.14 stops overriding models' sampler defaults

OpenAI-compatible endpoints now use a model's own temperature and top_p when a client sends none, instead of 1.0.

— GitHub, ollama/ollama v0.40.14, November 3
github.com/ollama/ollama/releases/tag/v0.40.14

THREATS

Kaspersky finds an LLM built into an attacker's C2 server

Attackers in schools let the CyberStrikeAI framework write post-exploitation commands; domain controllers fell in three to four days.

— Daily CyberSecurity, November 3
securityonline.info/cyberstrikeai-framework-attacks

KUBERNETES

k3s 1.37.2, 1.36.6 and 1.35.10 pre-releases bump x/net

Each carries one golang.org/x/net update, with no CVE named. Upstream patches target November 10.

— GitHub, k3s-io/k3s, November 3; kubernetes.io
github.com/k3s-io/k3s/releases

KUBECTL TIP

`kubectl rollout history deploy/web`

Revisions behind a Deployment *(kubernetes.io)*

KUBECTL TIP

`kubectl cluster-info dump`

Cluster state to stdout, for debugging *(kubernetes.io)*

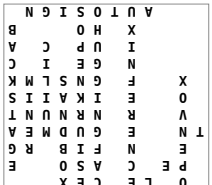
PUZZLE · WORD SEARCH

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

FIND AUTOSIGN · BACKSTAGE · CILIUM · FLEET · HUGGINGFACE · MINER · OPENKRUISE · OPENVOX · SANDBOX · XINFERENCE

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

Words run in every direction, also backwards.



SOLUTION