All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
0 days
to the OSC Kolkata CFP

VOL. I · NO. 309 THURSDAY, NOVEMBER 5, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ OPEN WEIGHTS
Moonshot's 2.8T open model is public now, under its own licence P.2

◆ CLOUD SECURITY
Mandiant: LLMjacking can run up over $100,000 in a day P.2

◆ DATA PIPELINES
Airbyte's 9.9 Connector Builder flaw is exploited, and 1.x gets no fix P.2

KUBERNETES SECURITY

Kyverno flaw rated 9.9 lets a tenant rewrite a neighbour's RoleBindings

CVE-2026-122313 was assigned this week; the fix is the 1.19.2 release of October 20. Older versions are exposed wherever tenants write policies.

COMPILED FROM GITHUB ADVISORIES, OCTOBER 21-23; VULNCHECK AND CVE WATCHTOWER, NOVEMBER 4-5

A tenant allowed to create a NamespacedMutatingPolicy names another namespace's RoleBinding in a CEL target expression, and the background controller patches it with its cluster-wide ServiceAccount, adding the attacker's subjects.

Roles, NetworkPolicies and ConfigMaps are reachable too. No exploitation is confirmed.

Sources differ: VulnCheck gives 1.17.0 up to 1.19.2, at 9.4 on CVSS 4.0. GitHub's October 21 advisory says up to 1.19.0, at 9.9 on CVSS 3.1, and lists no CVE.

What to do: upgrade to 1.19.2; its notes name no 1.18 or 1.17 fix. Otherwise restrict who can create these policies, then audit tenant RoleBindings.

Full story → github.com/kyverno/kyverno/security/advisories/GHSA-f96w-622v-rqpq
www.vulncheck.com/advisories/kyverno-1.17.0-before-1.19.2-cross-namespace-privilege-escalation-via-namespacedmutatingpolicy

WHAT KYVERNO 1.19.2 CLOSED

24 ADVISORIES IN ALL
14 HIGH
9 CRITICAL
1 MODERATE

Kyverno v1.19.2 release notes, October 20.

AI AND THE KERNEL

OpenAI's model reproduced 1,724 Linux kernel flaws and built root exploits for 948

The October run cost $1.21 million, about $1,279 per exploitable flaw, and scanned about 7% of the kernel's code.

COMPILED FROM DAILY CYBERSECURITY, NOVEMBER 5, ON OPENAI'S REPORT; THE NEURON, NOVEMBER 5

An unnamed upcoming OpenAI model ran a five-stage pipeline for about 10 days. Agents raised 2,308 candidates, reproduced 1,724 (74.7%) in isolated VMs with KASAN, then built 1,169 working root exploits, which map to 948 unique flaws.

Caveats: this is OpenAI's own account. Its report could not be read directly, so these figures come from Daily CyberSecurity; a second digest matches the headline numbers. In an early test, 20 of 200 claimed exploits triggered the wrong bug.

What to do: patch node kernels quickly, and sandbox untrusted workloads with gVisor or Firecracker.

Full story → securityonline.info/openai-cyber-model-linux-kernel-vulnerabilities
openai.com/index/a-thousand-fewer-paths-to-root

AI INFRASTRUCTURE

GPUStack's 9.8 login bypass is now exploited, with reverse shells on GPU hosts

COMPILED FROM GITHUB ADVISORIES; DAILY CYBERSECURITY, NOVEMBER 5

Loopback requests got admin rights, and a same-host proxy or a spoofed X-GPUStack-Real-IP header fakes that. The July 31 advisory says "observed exploited in the wild against a v2.1.1 deployment." Upgrade to 2.2.2, which also stops CVE-2026-102894 (9.1), a forged SAML login.

Full story → github.com/gpustack/gpustack/security/advisories/GHSA-gj9m-f8ph-pmhr
securityonline.info/gpustack-authentication-bypass-cve-2026-102895-exploited

LINUX SECURITY

APT root flaw means rebuilding base images

COMPILED FROM UBUNTU; DEBIAN; DAILY CYBERSECURITY, NOVEMBER 5

CVE-2026-109518 lets a rogue mirror or proxy swap a verified package when Acquire::Retries is non-zero, the default on Debian 12 and Ubuntu 22.04 onward. Canonical says 7.7, Debian's maintainer critical. No attacks are known. Fixed in Debian 2.6.2 and 3.0.4 and USN-8996-1; move sources to HTTPS.

Full story →
ubuntu.com/security/CVE-2026-109518
security-tracker.debian.org/tracker/CVE-2026-109518

GITOPS

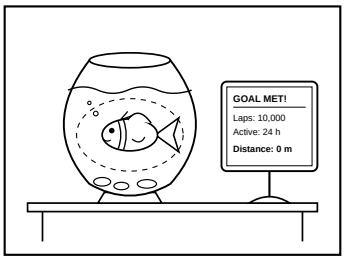
Argo CD 3.6 sends SSA apps through Server-Side Diff

COMPILED FROM ARGO CD UPGRADE GUIDE

Released November 3. Webhook rejections now show as diff errors. Rename ARGOCD_REPO_OTLP_HEADERS first. 3.3 is now end of life.

Full story → argo-cd.readthedocs.io/en/stable/operator-manual/upgrading/3.5-3.6

CARTOON OF THE DAY



Drawing: Claude

Personal best. Same bowl.

WHY IT'S FUNNY A goldfish in a sweatband hits its tracker's goal of 10,000 laps, and the screen shows the distance covered: zero. Some busy days end the same way.

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

Nov 9-12 EVENT
KubeCon + CloudNativeCon NA, Salt Lake City

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

authn and frontend add PKCE as snowplow 1.12.65 fixes a cache deadlock

November 5, 2026 — On November 4, authn stopped following redirects with credentials, PKCE reached the login paths, and a snowplow pre-release replaced 1.12.61–1.12.64, now marked do not install.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

snowplow 1.12.65 · Nov 4
- Pre-release: fixes cache deadlock #1146.

github.com/krateo-platformops/snowplow/releases

authn 0.33.1–0.35.3 · Nov 4
- Credentialed calls refuse redirects; roll 0.35.3.

github.com/krateo-platformops/authn/releases

core-provider 2.13.56–2.13.63 · Nov 4
- No CRD may get stricter; skip 2.13.61.

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

frontend, portal 1.8.20–1.8.23, 1.8.89–1.8.91 · Nov 4
- PKCE on OIDC login; tickets follow RBAC.

github.com/krateo-platformops/frontend/releases

provider-runtime, oasgen, alert, git 1.8.2, 0.51.0, 0.2.60, 0.16.0 · Nov 4
- Ready=Unknown when a resource is unobservable.

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

installer 0.3.497–0.3.506 · Nov 4
- incident-provider cutover; skip 0.3.505.

github.com/krateo-platformops/installer/releases

Latest elsewhere: observability 3.1.34 (Nov 3), sse-proxy 1.3.0 (Nov 1), otel-collector 1.0.4 (Oct 12), helm-render-service 0.5.0 (Sep 30).

KRATEO AGENTIKO

Merged into main this week

Krateo Agentiko notifications could not be read this morning.

NEWS IN BRIEF

OPEN WEIGHTS

Moonshot's 2.8T open model is public now, under its own licence

Yesterday we reported the Kimi K3.1 Pro weights as missing; the repository is now up, with 104B parameters active per token and a 1M context. Read the custom licence first.

— Hugging Face, moonshotai/Kimi-K3.1-Pro, November 5
huggingface.co/moonshotai/Kimi-K3.1-Pro

OPEN WEIGHTS

Ripple-65B Preview offers a dense Apache 2.0 model with a 1M context

Ricursive claims 80.5 on Terminal-Bench 2.1, just above Reflection Beam's 80.1. Scores are vendor-reported, and no inference provider hosts it yet.

— Hugging Face; The Neuron, November 5
huggingface.co/ricursiveAI/Ripple-65B-Preview

LLM RELEASES

Tencent's Hy4 adds vision and computer use at the preview's prices

It launched November 4 at $0.834 in and $2.501 out per million tokens. Weights are promised "shortly"; TechNode reports no benchmarks.

— TechNode, November 4
technode.com/2026/11/04/tencent-launches-hy4-with-vision-and-computer-use-capabilities

CLOUD SECURITY

Mandiant: LLMjacking can run up over $100,000 in a day

Some victims lost up to $1 million, and one service resold frontier access for about $60 a month. Set quotas and budget alerts, and patch LiteLLM's CVE-2026-40217.

— Daily CyberSecurity, November 4, on a Mandiant and GTIG report
securityonline.info/llmjacking-cloud-attacks-mandiant

DATA PIPELINES

Airbyte's 9.9 Connector Builder flaw is exploited, and 1.x gets no fix

JPCERT/CC warned on November 4. On 2.x any Workspace Reader can run code in the container. Upgrade to 2.2.0 and rotate stored credentials.

— Daily CyberSecurity, November 4
securityonline.info/airbyte-vulnerability-exploited

GPU CLOUD

NVIDIA rotates Brev SSH keys after an October intrusion

The intrusion ran October 4-20 and may have exposed customer VM keys; NVIDIA has seen no misuse. Check authorized_keys and rotate secrets on instances.

— Daily CyberSecurity, November 4
securityonline.info/nvidia-brev-security-incident

MIDDLEWARE

ZooKeeper 3.9.7 fixes a crash that can leave data "permanently unbootable"

Five flaws rated up to 8.7 include a SASL superuser bypass. Upgrade to 3.9.7; 3.8.8 lacks the multiRead fix.

— Daily CyberSecurity, November 5
securityonline.info/apache-vulnerabilities-zookeeper-openoffice-activemq

AI ON KUBERNETES

A CNCF guide puts NVIDIA's OpenShell agents on Agent Sandbox

OpenShell 0.1.3 denies egress by default; each agent needs a supervisor Pod. The demo pins Kyverno 1.18.2, in the lead's range. Nirmata member post.

— CNCF blog, November 4
www.cncf.io/blog/2026/11/04/openshell-on-kubernetes-a-guide-for-platform-engineers

CONTAINERS

Amazon ECS Gateway gives each service a generated hostname

One resource provisions a certificate and listener rule per service; no custom-domain path is documented.

— InfoQ, November 4
www.infoq.com/news/2026/11/introducing-amazon-ecs-gateway

KUBECTL TIP

`kubectl logs deploy/my-deployment`

Pod logs for a Deployment *(kubernetes.io)*

PUZZLE · WORD SEARCH

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

FIND AIRBYTE · ARGOCD · EXPLOIT · GPUSTACK · KERNEL · KYVERNO · MIRROR · ROLEBINDING · TENANT · ZOOKEEPER

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

Words run in every direction, also backwards.

SOLUTION

