All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
1 day
to the Platform Engineering CFP

VOL. I · NO. 294 WEDNESDAY, OCTOBER 21, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ AUTOSCALING
A namespace admin can send KEDA's own token to their URL, at 9.9 P.2

◆ CONTAINERS
One image annotation switches off Podman's sandbox, at 10.0 P.2

◆ INFERENCE ENGINES
DeepSeek open-sources DeepInfer, for one model and offline use only P.2

GITOPS SECURITY

A Kustomize ref runs commands in Argo CD's repo-server, at 9.9

CVE IDs landed October 20 for advisories first published October 7. Fixed in 3.3.15, 3.4.10 and 3.5.4; v2 from 2.7.0 gets no patch.

COMPILED FROM ARGO CD SECURITY ADVISORIES GHSA-9V9P-X54C-58GC AND GHSA-FW5C-W8RC-J7FX

Kustomize passes a remote resource's ref or version to git fetch without a "--" separator, so a value such as --upload-pack=<command> becomes a Git option. Over a file:// remote the command runs inside argocd-repo-server. CVE-2026-113708 needs only Application get, through the manifestsWithFiles endpoint.

The bug arrived when Argo CD moved to Kustomize 5.0.1, first shipped in 2.7.0. Its sibling, CVE-2026-113709, lets helmGlobals.configHome load a Helm downloader plugin from the repository when --enable-helm is set.

Upgrade to 3.3.15, 3.4.10, 3.5.4 or later. On v2, pin Kustomize below 5.0 per Application.

Continued on page 2

THE ARGO CD FLAWS IN FOUR NUMBERS

13 DAYS, ADVISORY TO CVE

5 KUSTOMIZE MAJOR TO AVOID

3 V3 LINES WITH A FIX

0 PATCHED V2 RELEASES

Both CVEs score 9.9. Advisories published October 7, CVE IDs October 20. Not in CISA KEV and no exploitation reported.

AI ON KUBERNETES

llm-d 1.0 makes multi-tenant inference the default problem, with a v1 config API

The CNCF Sandbox project shipped October 20. The adopter figures are the project's own.

COMPILED FROM LLM-D BLOG AND V1.0.0 RELEASE NOTES, OCTOBER 20

The router gains priority- and fairness-aware flow control that sheds load under saturation; defaults stay first-come-first-served. The Endpoint Picker gets a hot standby, and DisaggregatedSet upgrades prefill and decode in lockstep.

Google says Vertex AI cut time-to-first-token by more than 35% and doubled its prefix-cache hit rate to 70%. AWS reports up to 70% more tokens per second than plain vLLM. IBM Research serves 3,000 coding agents on 544 H100s.

The config API is now v1, flow control moves under flowControl, and LWS 0.11.1 or later is required.

Full story → llm-d.ai/blog/llm-d-v1.0-state-of-the-art-inference-ready-for-day-2 github.com/llm-d/llm-d/releases/tag/v1.0.0

TRUST STORES

Guessable keys get three emSign roots distrusted

Eight eMudhra intermediate keys were compromised; Mozilla knew on October 17.

COMPILED FROM DAILY CYBERSECURITY, OCTOBER 21, AND GITHUB ADVISORY GHSA-6Q48-6C7W-9GW2

The keys, from April 2025, could be recovered in 256 tries. NSS 3.131.1, Go 1.26.10 and certifi 2026.10.19 drop the roots. Rebuild images that vendor certifi or Go.

Full story → securityonline.info/emudhra-certificate-compromise-mozilla github.com/advisories/GHSA-6q48-6c7w-9gw2

SUPPLY CHAIN

OVHcloud CLI releases swapped for a secret stealer

Files in old GitHub releases were replaced on October 19.

COMPILED FROM DAILY CYBERSECURITY, OCTOBER 20

The Stack puts the range at v0.11.0 to v0.15.0. A customer's pinned SHA-256 check caught it; OVHcloud blocked it in 94 minutes. Rotate keys on affected machines.

Full story → securityonline.info/ovhcloud-cli-supply-chain-attack

DEVELOPER PORTALS

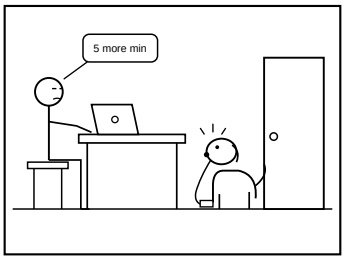
Backstage 1.56 needs a maintenance window

COMPILED FROM BACKSTAGE V1.56.0 RELEASE NOTES

One ingestion-table migration cannot run as a rolling upgrade. Database keepalive is now off by default; the Signals WebSocket needs a user token.

Full story → backstage.io/docs/releases/v1.56.0 github.com/backstage/backstage/releases/tag/v1.56.0

CARTOON OF THE DAY



Drawing: Claude

He brought the lead at minute one. It is now minute forty.

WHY IT'S FUNNY The dog has been sitting by the door with his lead in his mouth since the first "five more minutes". The human means it every time, and every time it is a lie. Dogs cannot read clocks, but they have learned exactly how long five human minutes really are.

DATES TO WATCH

Events and calls for papers

Oct 22 CFP
Platform Engineering 2026 (virtual, Nov 5): talks due

Oct 22 ONLINE
Advanced Kubernetes, LearnKube online course

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

Portal 1.8.75 drops tiers, 1.8.77 narrows the devs persona, and snowplow 1.12.51 closes a data leak

October 21, 2026 — Monday's releases change who sees what: sidebar namespaces now follow the caller's RBAC, devs lose their ClusterRole, and the installer prunes four cluster-scoped objects on upgrade.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

snowplow 1.12.51 · Oct 20

- Security: filtered responses no longer leak raw data on fail-closed paths.

github.com/krateo-platformops/snowplow/releases

portal 1.8.75 · Oct 20

- Breaking: tiers values removed; sidebar namespaces follow RBAC. 1.8.77 drops the devs ClusterRole.

github.com/krateo-platformops/portal/releases

installer 0.3.438 · Oct 20

- Breaking: pins portal 1.8.77 and prunes four devs-group cluster objects.

github.com/krateo-platformops/installer/releases

observability 3.1.19 · Oct 20

- Audit log pipeline into ClickHouse, 365-day TTL.

github.com/krateo-platformops/observability/releases

Latest elsewhere: frontend 1.8.9, installer 0.3.439 (Oct 20), core-provider 2.13.26 (Oct 19).

KRATEO AGENTIKO

Merged into main this week

No new Krateo Agentiko pull requests since the last issue.

CONTINUED FROM PAGE 1 · GITOPS SECURITY

Argo CD flaw

Blocking egress does not help: a file:// remote never leaves the pod.

Full story → github.com/argoproj/argo-cd/security/advisories/GHSA-9v9p-x54c-58gc github.com/argoproj/argo-cd/security/advisories/GHSA-fw5c-w8rc-j7fx

NEWS IN BRIEF

AUTOSCALING

A namespace admin can send KEDA's own token to their URL, at 9.9

CVE-2026-77524: an unvalidated hashiCorpVault.address in a TriggerAuthentication makes the KEDA operator send its cluster-wide ServiceAccount token to a tenant-controlled address. It is an incomplete fix of CVE-2025-68476. Published by the project September 23 and by NVD October 14; fixed in 2.21.0, with no workaround listed.

— GitHub advisory GHSA-637c-6jxx-4rwm
github.com/advisories/GHSA-637c-6jxx-4rwm

CONTAINERS

One image annotation switches off Podman's sandbox, at 10.0

CVE-2026-94603: an image carrying io.podman.annotations.checkpoint.runtime.name is treated as a checkpoint, and podman run ignores flags such as --cap-drop=ALL. Fixed in 5.8.8 and 6.1.3; rootless containers are not affected. Published September 29, in the GitHub database since October 15.

— GitHub advisory GHSA-2cvf-wqm6-wr9g
github.com/advisories/GHSA-2cvf-wqm6-wr9g

SECRETS

External Secrets Operator lost its webhook label check to an init-order bug

CVE-2026-26287, CVSS 7.1: EnforceLabels was cleared, so anyone who can create Webhook generators can send an unlabelled secret to an outside URL. Affects v0.10.0 to v1.3.1; fixed in v1.3.2 and v2.0.0. Advisory from October 6, in the Go database October 20.

— External Secrets advisory GHSA-q7hv-xx6h-q2x8
github.com/external-secrets/external-secrets/security/advisories/GHSA-q7hv-xx6h-q2x8

JAVA RUNTIMES

Tomcat fixes eight flaws, including HTTP/2 responses sent to the wrong user

Disclosed October 20: CVE-2026-101296 bypasses JNDIRealm authentication with non-GSSAPI SASL, and CVE-2026-101356 mixes up HTTP/2 requests and responses between users. Upgrade to 11.0.27, 10.1.61 or 9.0.123; 8.5 and 7.0 get nothing. Apache rates them Important, while CISA's scores reach 9.1.

— Daily CyberSecurity, October 21
securityonline.info/apache-tomcat-vulnerabilities-october-2026

INFERENCE ENGINES

DeepSeek open-sources DeepInfer, for one model and offline use only

Apache 2.0, running DeepSeek-V4.1-Flash on NVIDIA SM100 GPUs or Huawei Ascend 950 NPUs, with CUDA 13 or CANN 9.2. The README says a full service still needs a KV cache system, prefill/decode disaggregation and data-parallel load balancing, none of which ship.

— DeepInfer repository on GitHub
github.com/deepseek-ai/DeepInfer

KUBECTL TIP

`kubectl rollout status deploy/web`

Watch a rollout until it finishes *(kubernetes.io)*

ACCELERATORS

Hugging Face models now treat a TPU as just another PyTorch device

Published October 20: with TorchTPU, Transformers takes device_map="tpu" and Diffusers pipe.to("tpu"); Optimum TPU is no longer needed. 96.5% of Transformers tests that run on TPU pass, and MoE kernels decode 21.5x faster on Qwen3-30B-A3B at batch 64 on v6e-8, Hugging Face says.

— Hugging Face blog
huggingface.co/blog/hf-torchtpu

KUBECTL TIP

`kubectl logs -p -c ruby web-1`

Logs of the container that crashed *(kubernetes.io)*

PUZZLE · WORD SEARCH

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

FIND BACKSTAGE · CERTIFI · DEEPINFER · KEDA · KUSTOMIZE · OVHCLOUD · PODMAN · SNOWPLOW · TOMCAT · TORCHTPU

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

Words run in every direction, also backwards.



SOLUTION