All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
2 days
to the GENAIX Singapore CFP

VOL. I · NO. 286 TUESDAY, OCTOBER 13, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ CLOUD NATIVE SECURITY
Dapr 1.18.6 stops one app setting reminders on another app's actors P.2

◆ EXFILTRATION RISK
A tenant subdomain redirects SAP's OAuth2 token request, CVSS 10.0 P.2

◆ VIRTUALISATION
KubeVirt 1.9.1 puts back the old VFIO path for PCI passthrough P.2

PLATFORM ENGINEERING

AI doubled Spotify's merged changes to 17,000 a month

Reported October 12. Fleet Management has merged 2.5 million automated pull requests, and a background agent runs Claude in Kubernetes pods. Two incidents showed where the controls had not kept up.

COMPILED FROM INFOQ

Spotify went from about 8,100 merged code changes a month to roughly 17,000 in the year to August 2026, across nearly 3,000 production services. Fleet Management has merged over 2.5 million automated maintenance pull requests, and a background agent, Honk, runs Claude in Kubernetes pods.

The volume outran the verification. On June 24 a scheduled batch job competed with new podcast episodes in the ingestion pipeline; a scheduling bug cut throughput by about 10 per cent and episodes that publish in minutes were delayed by hours.

The remedies are platform work: end-to-end monitoring, batch jobs demoted, more rollback capacity, and automated changes scheduled inside the owning team's hours. The figures are Spotify's own and were not independently audited.

Full story → www.infoq.com/news/2026/10/spotify-ai-quality-controls

WHAT THE EXTRA CHANGES WERE

27	QUALITY WORK, 2025
31	QUALITY WORK, 2026
31	MAINTENANCE, 2025
25	MAINTENANCE, 2026

Share of merged changes, per cent, year on year to August 2026. Volume itself roughly doubled. Spotify reports no matching rise in rework, but says pull request size and code complexity are both increasing. Company-reported figures. Source: infoq.com.

AI ON KUBERNETES

vLLM lets decode hand the KV cache back: 2,334 ms down to 702 ms at 20k tokens

Posted October 12. In multi-turn agentic traffic the prefill node stops recomputing the previous turn. Benchmarked by AWS on H200s.

COMPILED FROM VLLM BLOG

Prefill-decode disaggregation moves the KV cache one way, so on the next turn prefill recomputes KV that decode already holds. The new path adds a reverse NIXL read, a router mapping conversation_id to decode's blocks, and two knobs: decoder_kv_blocks_ttl at 480 seconds and kv_recompute_threshold at 64 tokens.

On a 1P1D deployment GLM-5-FP8 time to first token fell from 2,334 ms to 702 ms at 20k prompt tokens; Qwen3-32B went 778 ms to 460 ms at 24k. Prefix caching was disabled on the prefill node to emulate eviction, which flatters the result.

Full story → vllm.ai/blog/2026-10-12-bidirectional-kvxfer-multiturn-agentic-workload

> ***"results depend on workload and configuration"***
>
> — VLLM BLOG, BI-DIRECTIONAL KV TRANSFER, OCTOBER 12, 2026

CLOUD NATIVE SECURITY

A regex compiler in GitLab CI gives unauthenticated code execution, CVSS 10.0

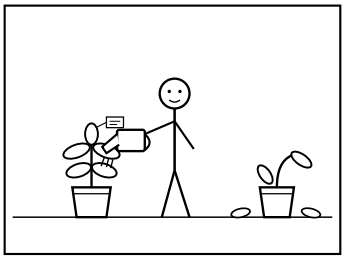
CVE-2026-97229, patched October 8. Weak validation overflows an integer; a crafted expression in a CI/CD config then runs code.

COMPILED FROM SECURITYONLINE.INFO

Affected: Community and Enterprise Edition 19.1 before 19.2.8, 19.3 before 19.3.4 and 19.4 before 19.4.2; the release closed 24 security issues. GitLab.com and Dedicated are patched, self-managed installs are not. Upgrade internet-facing instances first and rotate CI/CD secrets if anything looks wrong.

Full story → securityonline.info/gitlab-cve-2026-97229-arbitrary-code-execution

CARTOON OF THE DAY



Drawing: Claude

This one's thriving.

WHY IT'S FUNNY The plant being watered still has the shop tag hanging off it, because it is plastic. The real one in the next pot has dried out and dropped its leaves on the floor. The joke is the care we lavish on the thing that needs none, while the thing that needs it quietly gives up.

DATES TO WATCH

Events and calls for papers

Oct 13–16 ONLINE
OpenStack and OpenInfra Project Teams Gathering, virtual, running to Friday

Oct 15 ONLINE
KubeVirt Summit 2026, virtual and free

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

The portal stops pulling 15.3 MB to keep 49 KB

October 13, 2026 — Three components shipped on October 12: snowplow added the RBAC verb last week's refresher fix needed, the portal replaced a full CRD listing with per-group discovery, and the frontend fixed readyWhen in the preview.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

snowplow 1.12.43 · Oct 12

- Grants the impersonate verb in the chart, so the cohort-reading refresher fix takes effect in production.

github.com/krateo-platformops/snowplow/releases

portal 1.8.70 · Oct 12

- composition-events resolves plurals per API group: it was fetching 15.3 MB a call to keep 49 KB.

github.com/krateo-platformops/portal/releases

frontend 1.8.1 · Oct 12

- Composer's readyWhen evaluates correctly in the preview's jq; live refresh stops retrying HTTP 400s.

github.com/krateo-platformops/frontend/releases

Also Oct 12: observability 0.1.22, installer 0.3.417, sse-proxy 0.1.14, otel-collector 0.3.8. Latest elsewhere: alert-provider 0.2.49 (Oct 9), core-provider 2.13.23 (Oct 5).

KRATEO AGENTIKO

Merged into main this week

No new Krateo Agentiko pull requests since the last issue.

SUPPLY CHAIN

A fake AWS Terraform provider drops a Rust backdoor

terraform-provider-awsbeta, found by Zscaler ThreatLabz in July and written up October 12. It works as a provider, which is the point.

COMPILED FROM SECURITYONLINE.INFO, ZSCALER THREATLABZ

A bash loader runs when Terraform starts the plugin, then pulls a payload disguised as a web font. FLATROOF, a Rust backdoor, lifts browser passwords and shell history and drops ROOFDECK for reverse shells. Install providers only from the official registry or a trusted mirror, and verify checksums.

Full story → securityonline.info/tradertraitor-trojanized-terraform-provider

AGENTS ON KUBERNETES

kagent makes agents YAML; the guardrail is RBAC

CNCF blog, October 12. A Sandbox project; the walkthrough runs Helm chart 0.10.2 on kind.

COMPILED FROM CNCF

An Agent is a custom resource the controller turns into a pod speaking A2A. The builder agent gets three tools out of 22, read-only RBAC and approval on every apply. The authors warn the default is not shareable: auth runs unsecured and access is port-forwarding only.

Full story → www.cncf.io/blog/2026/10/12/from-zero-to-agent-builder-running-kagent-on-your-laptop

NEWS IN BRIEF

CLOUD NATIVE SECURITY

Dapr 1.18.6 stops one app setting reminders on another app's actors

Version 1.18.6 and the 1.17.16 backport, both October 9, are security releases, separate from the 1.18.5 bug-fix round. They stop spoofed caller identity headers reaching target apps and fix an ACL bypass through percent-encoded paths.

— GitHub · dapr
github.com/dapr/dapr/releases/tag/v1.18.6

GITOPS

3.5.5, 3.4.11 and 3.3.16 plug a goroutine leak left by failed plugins

Three new Argo CD point releases on October 12, bug fixes rather than the security round of October 6. They plug a goroutine leak after config management plugin failures, stop stale manifests being served, and fix OCI tag list caching.

— GitHub · argoproj
github.com/argoproj/argo-cd/releases/tag/v3.5.5

EXFILTRATION RISK

A tenant subdomain redirects SAP's OAuth2 token request, CVSS 10.0

CVE-2026-89111, from SAP's October 13 patch day, is unauthenticated SSRF in the SAP Cloud SDK for Python. An attacker controlling a tenant subdomain in a multi-tenant BTP app can redirect the OAuth2 token request; credentials can be exfiltrated. Update, then rotate.

— securityonline.info
securityonline.info/sap-security-patch-day-october-2026

VIRTUALISATION

KubeVirt 1.9.1 puts back the old VFIO path for PCI passthrough

Released October 12. It restores the legacy VFIO fallback for PCI passthrough, fixes a wrong VM status after a manual stop, and ignores memory overcommit for VMs on hugepages.

— GitHub · kubevirt
github.com/kubevirt/kubevirt/releases

KUBECTL TIP

`kubectl diff -f pod.json`

See what an apply would change first *(kubernetes.io)*

DATABASES

MariaDB's RPM packages put the mysql home inside the data directory

Nine flaws disclosed October 9. CVE-2026-107814, CVSS 8.4, means startup files in the data directory run when an admin opens a login shell; Debian is unaffected. Fixed in server 10.6.28, 10.11.19, 11.4.13, 11.8.9, 12.3.3 or 13.0.2.

— securityonline.info
securityonline.info/mariadb-vulnerabilities-privilege-escalation

ARCHITECTURE

Grab folded a counter's time buckets into one record and halved p99

Grab halved p99 read latency by moving to Aerospike.

— InfoQ
www.infoq.com/news/2026/10/grab-counter-aerospike-migration

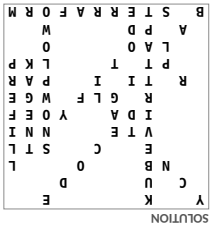
PUZZLE · WORD SEARCH

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

FIND DAPR · DECODE · GITLAB · KAGENT · KUBEVIRT · LATENCY · PREFILL · SNOWPLOW · SPOTIFY · TERRAFORM

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

Words run in every direction, also backwards.



SOLUTION