All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
2 days
to the Platform Engineering CFP

VOL. I · NO. 293 TUESDAY, OCTOBER 20, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ RELEASE CADENCE
Kubernetes 1.34 reaches end of life on October 27, and the October patch round is still missing P.2

◆ CONTAINER ESCAPE
A public exploit for an AF_UNIX use-after-free is still ahead of Canonical's kernel P.2

◆ SUPPLY CHAIN
Five minutes of tampering was enough to poison an update server P.2

CLOUD NATIVE SECURITY

Honeypots caught the Redis RESTORE flaw in use, and only 8.6.3 closes it

CVE-2026-25243 was disclosed in May. Defused's decoys logged scripted attacks on October 16 and 17, and CISA has not listed it.

COMPILED FROM DAILY CYBERSECURITY, FROM THE REDIS ADVISORY AND DEFUSED HONEYPOT DATA

RESTORE rebuilds a key from a serialized blob, and Redis does not fully validate that blob. A crafted payload can push the server into invalid memory access and, the advisory says, possibly remote code execution. The attacker must authenticate and must hold permission to run RESTORE, which is what a shared cache's credentials usually carry.

Defused logged repeated scripted attempts against its Redis decoys on October 16 and 17. One attacker hit a single decoy five times on a timer with the same payload, wiping the keyspace at the end of every run. EPSS puts exploitation at 3.3 per cent over 30 days.

The fix is Redis 8.6.3 or your distribution's patched package. If you cannot upgrade today, deny RESTORE with an ACL rule and get the service off any public address.

Full story → securityonline.info/redis-restore-cve-2026-25243-exploited

THE REDIS FLAW IN FOUR NUMBERS

9 CVSS IN THE AT-A-GLANCE BOX

5 MONTHS FROM ADVISORY TO ATTACK

5 REPEAT HITS ON ONE DECOY

3 EPSS, PER CENT OVER 30 DAYS

The write-up gives two severities, 7.7 in its summary and 8.8 in its at-a-glance box. Disclosed May 2026, attacks seen October 16-17, fixed in Redis 8.6.3.

OPEN MODELS

EmbeddingGemma 2 drops text, code, images, video and audio into one 768-dimension space

Apache 2.0, about 270 million parameters for text and code and about 740 million for the full multimodal set, reported October 19.

COMPILED FROM INFOQ, OCTOBER 19

Built on Gemma 4, open-weight under Apache 2.0 on Hugging Face. You load only the encoders you need: about 270 million parameters for text and code, about 740 million for all five modalities. Everything lands in the same 768-dimensional space, so a video clip and a sentence compare directly.

A million 768-dimensional vectors at bfloat16 take about 1.5 GB; truncated to 128 dimensions, about 250 MB. Retention is roughly 90 per cent for text but about 75 per cent for image, video and speech. Google publishes no benchmark scores.

Full story → www.infoq.com/news/2026/10/embeddinggemma-2-multimodal

PLATFORM ENGINEERING

The autoscaler never joined the DRA conversation, and that is where GPUs sit idle

A CNCF member post by AWS staff, October 19, on the seam between the scheduler and the cluster autoscaler.

COMPILED FROM CNCF BLOG, MEMBER POST BY AWS

Dynamic Resource Allocation replaced bare device counts with structured claims that describe topology, such as an accelerator plus the NIC that feeds it. The scheduler understands those claims; the au-

Continued on page 2

INGRESS SECURITY

A Traefik TLS-option cache hit skipped the cross-namespace check, and the databases disagree on how bad

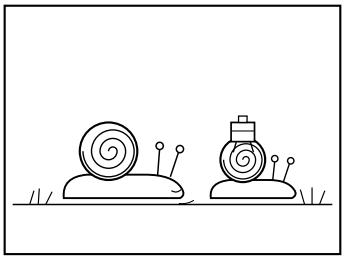
COMPILED FROM TRAEFIK SECURITY ADVISORIES ON GITHUB, PLUS THE CVE RECORD

GHSA-28hp-c82p-8vqj, which Traefik rates Low, says a TLS-option cache hit skips the cross-namespace authorization check, so an Ingress can use another namespace's CA secret. GHSA-p8wx-ph99-xgcr, High the same day, silently disables ingress-nginx mTLS when a sibling Ingress lacks the annotation.

CVE-2026-112778 covers the same reference. VulDB calls it critical, two databases score it 6.4.

Full story → github.com/traefik/traefik/security/advisories

CARTOON OF THE DAY



Drawing: Claude

Marco is doing the whole garden this year.

WHY IT'S FUNNY Two garden snails have met on the path, and one of them is wearing a backpack, which for a snail is the only possible sign of a long journey. The garden is perhaps three metres across, so the trip will still take him most of the summer. His friend is treating it as a gap year because, at that speed, it is one.

DATES TO WATCH

Events and calls for papers

Oct 20-22 EVENT
All Things Open, Raleigh, and TechEx Europe, Amsterdam

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

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

Nine releases on October 19 close a snowplow credential leak and rebuild oasgen-provider's CRDs

October 20, 2026 — A busy Sunday across the stack: snowplow 1.12.50 stops the /call passthrough forwarding the caller's credentials after a redirect, and oasgen-provider 0.32.0 starts reading path-item parameters.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

snowplow 1.12.50 · Oct 19

- Security: the /call passthrough no longer forwards the caller's credentials after a redirect.

github.com/krateo-platformops/snowplow/releases

oasgen-provider 0.32.0 · Oct 19

- Breaking: path-item parameters are now read, and required ones become required CRD fields, so existing CRs can fail admission.

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

Latest elsewhere: core-provider 2.13.26, installer 0.3.434, portal 1.8.74, frontend 1.8.7, observability 0.1.23 and alert-provider 0.2.50, all Oct 19. Deploy frontend-crd 1.8.6 before portal 1.8.74.

KRATEO AGENTIKO

Merged into main this week

No new Krateo Agentiko pull requests since the last issue.

CONTINUED FROM PAGE 1 · PLATFORM ENGINEERING

Autoscaler seam

toscaler, the post argues, still only answers whether to add a node.

Workload-aware scheduling is beta and off by default, and the autoscaler takes no part: it can add a node for a few pending gang members and strand the rest.

Full story → www.cncf.io/blog/2026/10/19/how-ai-workloads-are-reshaping-kubernetes-autoscaling

CI AND DELIVERY

Buildkite scopes a secret to one pipeline, one branch and one queue

Announced October 19: pipeline-scoped cluster secrets, token redaction in agent 4.0.9 and a validate_pipeline tool in the MCP server.

COMPILED FROM INFOQ, OCTOBER 19

A secrets view under Pipeline settings creates cluster secrets limited to one pipeline, narrowed further by branch, queue, build source or creator. Agent 4.0.9 redacts Buildkite tokens by prefix in job logs. In MCP server 1.23.0, create_webhook became a required parameter of create_pipeline, a breaking change.

Full story → www.infoq.com/news/2026/10/buildkite-ci-secrets-agentic

NEWS IN BRIEF

RELEASE CADENCE

Kubernetes 1.34 reaches end of life on October 27, and the October patch round is still missing

1.34 entered maintenance mode on August 27 and its last patch, 1.34.12, shipped September 23. The patch page targeted 1.37.2, 1.36.6 and 1.35.10 for October 13, but GitHub still shows 1.37.1, 1.36.5 and 1.35.9 as newest. Plan the move now.

— kubernetes.io patch releases and GitHub releases

kubernetes.io/releases/patch-releases
github.com/kubernetes/kubernetes/releases

CONTAINER ESCAPE

A public exploit for an AF_UNIX use-after-free is still ahead of Canonical's kernel

CVE-2026-80521 is a race in the kernel's AF_UNIX garbage collector that takes an unprivileged container process to root on the host, CVSS 7.8. The upstream fix landed August 6, but DepthFirst published a working exploit on September 22 and Canonical's 26.04 and 24.04 main kernels still read "work in progress". September news, not this week.

— Linux Journal, from Canonical's CVE tracker and DepthFirst

www.linuxjournal.com/content/ubuntu-container-escape-vulnerability-gets-public-exploit-kernel-patch-arrives

KUBECTL TIP

`kubectl api-resources`

Every resource kind the cluster knows *(kubernetes.io)*

EXPLOITED IN THE WILD

Plex2Shell went from proof of concept to cryptominers in a day

Zach Main published the four-CVE chain on October 16; honeypot attacks began October 17, with XMRig and a proxy tool served from one host. The chain steals the owner's admin token and runs commands as the Plex service user. Fixed in 1.43.3.10861.

— Daily CyberSecurity

securityonline.info/plex2shell-plex-media-server-exploited

SUPPLY CHAIN

Five minutes of tampering was enough to poison an update server

Google Threat Intelligence confirmed windows of ten minutes on May 28, six on July 16 and five on July 20 in which AOMEI's update servers served a trojanized archive, then clean files again. The clients never verified two remote config files, so no software bug was needed.

— Daily CyberSecurity, from Google Threat Intelligence

securityonline.info/aomei-supply-chain-attack-unc7017

WEB PLATFORM

Drupal's Field UI ran whatever callable a table row named

SA-CORE-2026-014 was patched October 14 and FORTBRIDGE published lab exploit code this week.

— Daily CyberSecurity, from the Drupal advisory

securityonline.info/drupal-rce-cve-2026-108097-poc

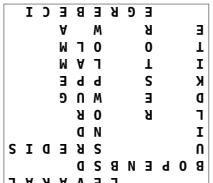
PUZZLE · WORD SEARCH

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

FIND **BUILDKITE · DRUPAL · GEMMA · ICEBERG · LARAVEL · OPENBSD · REDIS · RESTORE · SNOWPLOW · TRAEFIK**

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

Words run in every direction, also backwards.



SOLUTION