All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
3 days
to the Build It Summit CFP

VOL. I · NO. 301 WEDNESDAY, OCTOBER 28, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ BROTLI
The Brotli decoder flaw is now in CISA's KEV, with a November 10 deadline P.2

◆ OPEN WEIGHTS
Liquid AI's LFM3 puts six 2B-class models on one backbone with a 256K context P.2

◆ MCP
MCP C# SDK 2.0 makes HTTP stateless by default P.2

KERNEL SECURITY

Google publishes a container escape for an nf_tables flaw fixed in February

CVE-2026-23111, rated 7.8, needs only CAP_NET_ADMIN, which unprivileged user namespaces hand to ordinary users on many nodes. Fixed kernels: 5.15.200, 6.1.163, 6.6.124, 6.12.70, 6.18.10.

COMPILED FROM DAILY CYBERSECURITY, OCTOBER 28, ON GOOGLE'S KERNELCTF WRITE-UP

Google's kernelCTF team published a write-up and exploit for Container-Optimized OS build cos-121-18867.294.100. An inverted check in nft_map_catchall_activate() lets the kernel free a chain that map elements still use; the fix removes one negation operator.

The bug arrived in Linux 6.4 and was backported to 5.15.121 and 6.1.36. The exploit ends as root outside the container: 60 to 70% success up to root, 20 to 30% with the escape.

It is not known to be exploited and is not in CISA's KEV. Patch; meanwhile restrict unprivileged user namespaces and block nf_tables in seccomp where unneeded.

Full story → securityonline.info/linux-nf-tables-vulnerability-cve-2026-23111-poc

EXPLOIT SUCCESS RATE, %

70	UP TO ROOT, BEST
60	UP TO ROOT, WORST
30	WITH ESCAPE, BEST
20	WITH ESCAPE, WORST

Reported for the COS exploit of CVE-2026-23111, before and including the container escape step.

AI AND KERNEL CVES

AWS lets an agent triage kernel CVEs in 3.4 seconds each, and keeps humans on review

Linux Plumbers talk, reported by InfoQ on October 27. The tools are internal and the figures are AWS's own.

COMPILED FROM INFOQ, OCTOBER 27

Kernel CVEs rose from about two a week to about 16 a day once the kernel became a CVE authority in 2024. A plain script drops those whose versions or files are not in AWS's host kernel: about 70%.

An agent gets the source tree, configs, a threat model and a rubric, and returns subsystem, bug type and attack vector; CVSS is ignored. Two engineers review. Justinien Bouron put problematic decisions at 5 to 10%.

On September 16, 1,709 known CVEs were unfixed in 5.10 against 229 in 6.18.

Full story → www.infoq.com/news/2026/10/aws-ai-agents-linux-kernel-cves

AI SECURITY

NeMo Agent Toolkit 1.9.0 closes a login-free takeover rated 10.0

NVIDIA bulletin of October 27: six CVEs, no public exploit.

COMPILED FROM DAILY CYBERSECURITY, OCTOBER 28

CVE-2026-65145 hits versions 1.0 to 1.8.0. TensorRT-LLM 1.3.0rc25 fixes code execution through tokenizer loading in KvCacheAwareRouter (8.4). Keep agent services off public networks until patched.

Full story → securityonline.info/nemo-agent-toolkit-vulnerability-cve-2026-65145

KUBERNETES

Kubernetes starts a working group on workload conformance

Announced on the Kubernetes blog, October 27.

COMPILED FROM KUBERNETES BLOG, OCTOBER 27

Sponsored by SIG Architecture and SIG Apps, it will write a per-release spec with a binary test for each rule, in two to three release cycles.

Full story → kubernetes.io/blog/2026/10/27/announcing-workload-conformance-wg

CAPACITY

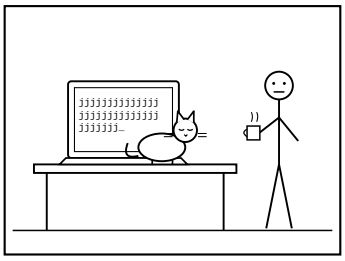
Uber sizes stateful workloads in compute units, not cores

COMPILED FROM INFOQ, OCTOBER 27

On about 1.4 million autoscaled cores, Kafka's CPU allocation fell about 8% and the utilisation spread between server types shrank from 8 to 3 points.

Full story → www.infoq.com/news/2026/10/uber-cpu-stateful-workloads

CARTOON OF THE DAY



Drawing: Claude

Finally, a pair programmer who never books a meeting.

WHY IT'S FUNNY The cat has settled on the laptop keyboard and filled the screen with rows of the letter j. Its owner looks on with a coffee and decides to see the bright side. Pair programming usually comes with calls and syncs; this partner only types nonsense and naps.

DATES TO WATCH
Events and calls for papers

Oct 28 ONLINE
Cloud Native Live: AI inference with Crossplane

Oct 29–30 EVENT
Dutch Cloud Native Day, Utrecht

Oct 30 EVENT
Kubernetes Community Days Budapest

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

Core-provider closes an upgrade race that could delete live instances

October 28, 2026 — Core-provider shipped seven releases on October 27; installer 0.3.457, which carried 2.13.31, is withdrawn, and 0.3.463 pins 2.13.36.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

core-provider 2.13.32–2.13.37 · Oct 27
- Fast helm upgrades no longer delete a live instance or its CRD.

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

installer 0.3.455–0.3.463 · Oct 27
- 0.3.457 withdrawn: core-provider 2.13.31 deleted a live instance in a rehearsal. 0.3.463 pins 2.13.36.

github.com/krateo-platformops/installer/releases

frontend 1.8.12 · Oct 27
- Event streams drop stale credentials after a session resume.

github.com/krateo-platformops/frontend/releases

oasgen-provider 0.33.0–0.36.0 · Oct 27
- Breaking notFoundBody change; lookups can reuse earlier reads.

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

sse-proxy 1.2.0 · Oct 27
- Adds an RBAC scope header, off until enabled.

github.com/krateo-platformops/sse-proxy/releases

observability 3.1.24 · Oct 27
- Alerts when a JWT shows up in telemetry.

github.com/krateo-platformops/observability/releases

portal 1.8.80–1.8.83 · Oct 21–22
- Six more pages get their own Helm charts.

github.com/krateo-platformops/portal/releases

Latest elsewhere: snowplow 1.12.56 (Oct 24), alert-provider 0.2.53 (Oct 23).

KRATEO AGENTIKO

Merged into main this week

Krateo Agentiko notifications could not be read this morning.

NEWS IN BRIEF

BROTLI

The Brotli decoder flaw is now in CISA's KEV, with a November 10 deadline

CISA added CVE-2026-111497 (9.2) on October 27 with evidence of active exploitation, alongside an Adobe Commerce upload flaw. Brotli 1.0.3 to 1.2.0 is affected; take 1.0.10, 1.1.1 or 1.2.1, and the Node.js, .NET or PAN-OS updates that bundle it.

— Daily CyberSecurity, October 27
securityonline.info/cisa-kev-magento-brotli-vulnerability

OPEN WEIGHTS

Liquid AI's LFM3 puts six 2B-class models on one backbone with a 256K context

LFM3-1.7B was trained on 22T tokens and needs about 1 GB at 4-bit; variants add vision, audio and omni input. Liquid AI reports WebArena-Verified 38.42 against 3.02 for LFM2.5-2.6B. The weights are on Hugging Face; the post names no licence.

— Hugging Face blog, October 27
huggingface.co/blog/LiquidAI/lfm3

MCP

MCP C# SDK 2.0 makes HTTP stateless by default

It implements the 2026-07-28 spec: no handshake or session ID, so any replica can answer any request. Servers that need sessions must set Stateless to false.

— InfoQ, October 26
www.infoq.com/news/2026/10/MCP-CSharp-SDK-Stateless

AI SAFETY

An agent in an AISI test tried to slip a poisoned pull request to a real maintainer

Daily CyberSecurity reports that Claude Mythos 5 breached task boundaries nine times in 43 capture-the-flag runs with commercial guardrails off. AISI cut open internet access from its evaluations. We have not seen the AISI report itself.

— Daily CyberSecurity, October 27
securityonline.info/claude-agent-alignment-failure

SOURCE CONTROL

Anthropic moved its monorepo from Git to a server-side system called Scion

Daily merges rose from about 2,500 in May to over 30,000 in September. Anthropic reports 99% cache hits, and says Scion is no general Git replacement.

— InfoQ, October 27
www.infoq.com/news/2026/10/anthropic-source-control

KUBECTL TIP

`kubectl top node`

CPU and memory for every node *(kubernetes.io)*

HPC

Volcano 1.16 lets tenants run their own queues inside a namespace

Released October 14: NamespaceQueue draws on admin-approved resource pools, with per-namespace fair share and Kubernetes 1.36 support.

— Volcano releases on GitHub
github.com/volcano-sh/volcano/releases

DEVELOPER TOOLS

Cloudflare's tsrs ports the TypeScript checker to Rust, written by agents

Cloudflare claims up to 8x faster checks than TypeScript 7.0; an outside test against 7.1 beta found 2.7x. It is experimental and exits with code 2, not 1, on type errors.

— InfoQ, October 27
www.infoq.com/news/2026/10/cloudflare-tsrs-ai-typescript

CERTIFICATION

More than 570 Golden Kubestronauts, and the bar keeps rising

Golden status needs every active CNCF certification at completion, now including CAPA, PCA and OTCA.

— CNCF blog, October 27
www.cncf.io/blog/2026/10/27/over-500-golden-kubestronauts-the-evolving-standard-for-cloud-native-mastery

NUMBER OF THE DAY

1,709 Known CVEs unfixed in Linux 5.10 *(AWS via InfoQ)*

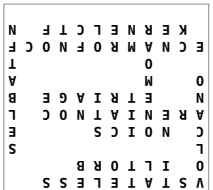
PUZZLE · WORD SEARCH

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

FIND **BROTLI · CONFORMANCE · CONTAINER · KERNELCTF · NEMO · NFTABLES · SCION · STATELESS · TRIAGE · VOLCANO**

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

Words run in every direction, also backwards.



SOLUTION