All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
0 days
to the CN AI + Inference CFP

VOL. I · NO. 292 MONDAY, OCTOBER 19, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ NODE IMAGES
Talos 1.14.4 already carries one of the fixed kernels P.2

◆ SUPPLY CHAIN
Chainguard puts each coding agent in its own microVM P.2

◆ CLOUD OPERATIONS
AWS puts the Well-Architected review behind an agent P.2

CLOUD NATIVE SECURITY

A guest can write into the host kernel through a deferred checksum, at 9.3

CVE-2026-99999, called PwnEscape, went public on October 19. Every kernel from 2.6.27 is affected and there is no workaround.

COMPILED FROM DAILY CYBERSECURITY, FROM THE KERNEL CVE RECORD AND THE ALMALINUX ADVISORY

Linux can defer a checksum calculation until late in the send path. A guest can influence the metadata that decides where that deferred write lands, and it can land inside an IPv4 header the kernel has already validated. Different code paths then trust different versions of the same packet.

The first effect is a leak of 32 bytes of host memory per packet. The researchers used it to plan writes into host kernel memory and ran a root helper on the host in their own KVM lab. No exploit code is out; EPSS puts exploitation at 0.2 per cent over 30 days.

The fix is in 5.10.272, 5.15.223, 6.1.190, 6.6.159, 6.12.113, 6.18.57 and 7.2.11. Drain and reboot multi-tenant nodes, sandbox platforms and CI runners first, and migrate guests off a host before rebooting it.

Full story → securityonline.info/pwnescape-linux-kernel-vm-escape-cve-2026-99999

THE PATCH YOU NEED, BY LINE

190 6.1 LINE, FIXED AT PATCH

159 6.6 LINE, FIXED AT PATCH

113 6.12 LINE, FIXED AT PATCH

57 6.18 LINE, FIXED AT PATCH

Also fixed: 5.10.272, 5.15.223 and 7.2.11. Anything older on your nodes is affected, back to 2.6.27. Source: the kernel CVE record for CVE-2026-99999.

AI ON KUBERNETES

vLLM 0.32.0 halves KV memory on SM100, and closes CORS by default

Released October 18, with seventeen breaking changes, three security advisories and a default that stops browser clients on upgrade.

COMPILED FROM VLLM V0.32.0 RELEASE NOTES, GITHUB

GLM-5.x now defaults to an FP8 KV cache on SM100 with --kv-cache-dtype auto, halving KV memory per rank. The project's benchmark puts the cost at 7 to 11 per cent on time-to-first-token and the gain at 2.3 to 5.5 per cent on throughput. On SM90, fp8_ds_mla gives GLM-5.3-Flash up to 31 per cent more output throughput.

With --api-server-count above 1, routing to the least-loaded API worker is worth 43 to 85 per cent more requests a second on short requests.

Read the breaking changes first. Python 3.10 is gone, cascade attention is removed, and max_tokens is now an upper bound on output rather than a reservation from the context window.

Full story → github.com/vllm-project/vllm/releases/tag/v0.32.0

LINUX KERNEL

Six more kernel flaws the same morning, five of them with a working root PoC

Hyunwoo Kim's "Infinity Core" set went public on October 19, hours from PwnEscape and in code every container shares.

COMPILED FROM DAILY CYBERSECURITY, FROM HYUNWOO KIM'S OSS-SECURITY POST

CVE-2026-98260 (7.8) is a use-after-free in CPU timers when exec() fails in a multi-threaded process, present

Continued on page 2

SOVEREIGN CLOUD

AWS unplugs its European Sovereign Cloud from the global backbone on Saturday

A deliberate disconnection of several hours on October 24, with traffic on European ISP links.

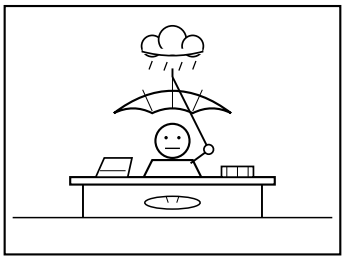
COMPILED FROM INFOQ, OCTOBER 18

AWS will cut the region off from the AWS Global Network, the private backbone carrying operational data between AWS locations, so traffic falls back to the public internet over the region's own links.

The region runs from Brandenburg, Germany. AWS expects short disruptions while routes converge and says the result can go into a compliance package for the EU Cloud Sovereignty Framework and BSI C3A.

Full story → www.infoq.com/news/2026/10/aws-sovereign-cloud-exercise

CARTOON OF THE DAY



Drawing: Claude

Facilities says the ceiling is a known issue.

WHY IT'S FUNNY A small rain cloud has formed indoors, directly over one desk, and the only person affected has simply opened an umbrella and carried on working. Nobody has fixed the ceiling, because it has been written down somewhere as known, and a known problem feels halfway to a solved one. The coffee cup stays out in the rain.

DATES TO WATCH

Events and calls for papers

Oct 19 CFP
Cloud Native AI + Inference Day Europe (Barcelona, Mar 15, 2027) and Cloud Native Days LA (Apr 1, 2027): talks due today

Oct 19 EVENT
Kubernetes Community Days UK, Edinburgh

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

installer 0.3.429 carries the core-provider policy fix into the chart

October 19, 2026 — One new release on October 18: the installer pins core-provider 2.13.25, the build that moved both chart templates to JSON Patch so Quantity strings stop being refused at admission.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

installer 0.3.429 · Oct 18

- Bumps core-provider and its CRDs from 2.13.24 to 2.13.25, delivering the JSON Patch fix from issue #66 to the chart.

github.com/krateo-platformops/installer/releases

frontend 1.8.5 · Oct 14

- List rows with only optional fields now open by default, and the Review step and the confirm dialog share one YAML display.

github.com/krateo-platformops/frontend/releases

Latest elsewhere: snowplow 1.12.49 (Oct 15), core-provider 2.13.25 and portal 1.8.72 (Oct 14), observability 0.1.22 (Oct 12).

KRATEO AGENTIKO

Merged into main this week

No new Krateo Agentiko pull requests since the last issue.

CONTINUED FROM PAGE 1 · LINUX KERNEL

Infinity Core

since 5.7 and fixed in 6.6.158, 6.12.112, 6.18.54 and 7.2.8. CVE-2026-89754 writes out of bounds in the page table walker behind mincore().

Five of the six give local privilege escalation, and the public proofs of concept turn them into a root shell. Restricting user namespaces or BPF does not block them.

Full story → securityonline.info/linux-kernel-vulnerabilities-infinity-core-poc

DATA PLATFORM SECURITY

Apache Kylin ships 12 fixes, and Airflow's SSH provider never checked host keys

Fifteen CVEs disclosed October 16, written up October 19.

COMPILED FROM DAILY CYBERSECURITY, FROM THE APACHE ADVISORIES

Kylin 4.0.0 through 5.0.4 are affected and 5.0.5 is the fix. CVE-2026-64959 is an unauthenticated backend cache API that accepts injected SQL; CVE-2026-108743 injects OS commands through Spark jobs.

In Airflow, CVE-2026-94134 (CISA scores it 9.1) means the SSH and SFTP providers skipped host-key checks. Upgrade that provider to 7.0.0 and set explicit host keys.

Full story → securityonline.info/apache-kylin-vulnerabilities-airflow-answer

NEWS IN BRIEF

NODE IMAGES

Talos 1.14.4 already carries one of the fixed kernels

Sidero Labs shipped Talos 1.14.4 on October 16 with Linux 6.18.57, pinning Kubernetes images to v1.37.1 and etcd to 3.7.2. 6.18.57 is the fixed stable release for the PwnEscape flaw. The day before, 1.14.3 took TimeService/TimeCheck away from the os:reader role.

— Sidero Labs releases
github.com/siderolabs/talos/releases

VULNERABILITY FEEDS

5,499 new CVEs in one week, and KEV trailed one of them by eight days

CVE Watchtower logged 5,499 new vulnerabilities between October 12 and 18, up from 3,255: 395 critical and 2,427 high. Daily CyberSecurity flagged Atlassian's CVE-2026-21589 on October 7; CISA added it to KEV on October 15. It is the publisher's own feed-to-feed tally.

— Daily CyberSecurity weekly CVE report
securityonline.info/weekly-cve-report-oct-12-18-2026

POLICY ENGINES

Kyverno 1.19.2-rc.2 drops kyverno-json and hardens the apiCall egress path

The candidate tagged October 17 removes kyverno-json from the test API, the JSON scan command and the Go module references, and bumps oras-go (CVE-2026-50163), the Go toolchain (CVE-2026-56853) and miekg/dns (CVE-2026-46600). It also hardens the apiCall.service egress path.

— Kyverno releases
github.com/kyverno/kyverno/releases

SUPPLY CHAIN

Chainguard puts each coding agent in its own microVM

Reported October 16: Workspaces gives a developer or an agent a hardened microVM, and a host-side proxy attaches short-lived credentials so no long-lived secret sits in the guest. Checks runs CI steps in warm microVMs and signs an attestation tied to environment, result and commit SHA.

— InfoQ; vendor announcement
www.infoq.com/news/2026/10/chainguard-workspaces-checks

KUBECTL TIP

`kubectl drain my-node`

Empty a node before the kernel reboot *(kubernetes.io)*

CLOUD OPERATIONS

AWS puts the Well-Architected review behind an agent

Announced October 18, it ranks findings on cost, security, performance and reliability across more than 65 AWS services, reading configuration, utilisation, topology and declared business goals. Preview runs in three US regions and needs Business Support or higher.

— InfoQ
www.infoq.com/news/2026/10/aws-well-architected-agent

KUBECTL TIP

`kubectl top node`

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

NUMBER OF THE DAY

32 bytes of host memory leaked per packet by PwnEscape *(Daily CyberSecurity)*

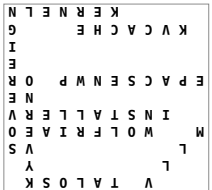
PUZZLE · WORD SEARCH

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

FIND **AIRFLOW · CHECKSUM · INSTALLER · KERNEL · KVCACHE · KYVERNO · PWNESCAPE · SOVEREIGN · TALOS · VLLM**

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

Words run in every direction, also backwards.



SOLUTION