All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
7 days
to the Build It Summit CFP

VOL. I · NO. 297 SATURDAY, OCTOBER 24, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ CERTIFICATES
cert-manager 1.21.3 stops copying a private key from a Secret the Certificate does not own P.2

◆ SIEM
Horizon3 publishes a working exploit for the FortiSIEM gRPC path traversal P.2

◆ OPENSTACK
Manila let other projects change a public share's access rules P.2

PHP RUNTIME

A third PHP flaw lands after PHP2Shell, and the October 21 patches miss it

CVE-2026-115560 needs a rare setup: turn off session upload progress. Images below PHP 8.4.27 or 8.3.36 still need a rebuild.

COMPILED FROM PHP VIA CANADIAN CENTRE FOR CYBER SECURITY ALERT AL26-026, AWS BULLETIN 2026-143, TANIUM, DAILY CYBERSECURITY

PHP 8.2.35, 8.3.36, 8.4.27 and 8.5.12 (October 21) fix CVE-2026-109618 and CVE-2026-109619, both 9.2 in CVSS v4, in FPM, mod_php, CGI, FrankenPHP and LiteSpeed. CVE-2026-115560, disclosed October 23, is not fixed.

Sources disagree: Tanium cites watchTowr honeypot hits; Canada's Cyber Centre and AWS confirm no attacks. VulnCheck got code execution on ARM64, and on x86 only with ASLR off. PAN-OS and Okta's gateway are patching.

Rebuild images from patched tags. Set session.upload_progress.enabled=0. PHP 8.1 and older: migrate.

Full story → cyber.gc.ca/en/alerts-advisories/al26-026-critical-vulnerabilities-impacting-php-cve-2026-109618-cve-2026-109619 aws.amazon.com/security/security-bulletins/2026-143-aws securityonline.info/php-session-vulnerability-cve-2026-115560

PHP2SHELL IN FOUR NUMBERS

10 EOL BRANCHES, NO FIX
9 HOURS OF WAF HEAD START
5 PAN-OS HOTFIX LINES
4 PHP BRANCHES PATCHED

EOL: 5.4 to 8.1. WAF: Cloudflare rules before disclosure, via Endor Labs.

GPU PLATFORMS

Three pods share one simulated A100 across Kamaji tenants, and a fourth is refused

CNCF blog, October 23: Kamaji tenants and HAMi's mock GPU plugin on one 4-core, 8 GB host.

COMPILED FROM CNCF BLOG, ANISH BISTA, OCTOBER 23

Kamaji runs each tenant's control plane as a pod; HAMi lets pods ask for GPU slices in megabytes and percent of compute. Tenant A got a simulated A100 (81,920 MB), tenant B two L4s, on Kubernetes 1.36.4.

Three pods asking for 20,000 MB and 30% each shared the A100. A fourth stayed Pending with CardInsufficientCore. Each tenant saw only its own GPUs; all eight tests passed.

HAMi's webhook must be reachable through Konnectivity, or GPU pods fall back to the default scheduler. No real memory enforcement or CUDA runs were tested.

Full story → www.cncf.io/blog/2026/10/23/multi-tenant-gpu-kubernetes-on-simulated-hardware-with-kamaji-and-hami

AI SECURITY

An LLMjacking agent turns exposed model endpoints into scanners and miners

Symantec's AI honeypot logged 127,000 requests.

COMPILED FROM SYMANTEC VIA DAILY CYBERSECURITY, OCTOBER 24

About 74 tools, from FOFA scans to cloud metadata SSRF, then XMRig. Require auth on model servers and MCP.

Full story → securityonline.info/skynet-llmjacking-agent

POLICY

Kyverno 1.19.2 closes 24 advisories, nine critical

Final release, October 20.

COMPILED FROM KYVERNO RELEASES ON GITHUB

Fixes cover apiCall paths, mutating-policy targets and image verification. Test first.

Full story → github.com/kyverno/kyverno/releases/tag/v1.19.2

OPENSTACK

Two Ironic flaws reach maintenance mode and the BMC

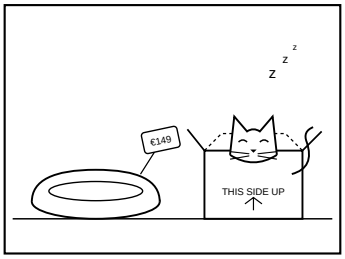
October 22; found by Metal3.io.

COMPILED FROM OPENSTACK SECURITY ADVISORIES

Lessees could set maintenance; Redfish passthru reached any BMC path.

Full story → security.openstack.org/ossa/OSSA-2026-048.html

CARTOON OF THE DAY



Drawing: Claude

We bought the orthopaedic memory-foam bed. She chose the box it came in.

WHY IT'S FUNNY The expensive cat bed sits empty with its price tag still on, while the cat is squeezed happily into the cardboard box it was delivered in. Every cat owner knows the box always wins. The more you spend on the present, the more the packaging is appreciated.

DATES TO WATCH

Events and calls for papers

Oct 24 EVENT
Kubernetes Community Days Nigeria (Lagos) and Indonesia (Bandung)

Oct 27 EVENT
Cloud Native Days Norway, Bergen

Oct 28 ONLINE
Cloud Native Live: AI inference with Crossplane

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

Core-provider stops caching CRD schemas per controller; snowplow narrows prewarm

October 24, 2026 — Five PlatformOps components shipped on October 23: core-provider 2.13.27 watches CRDs metadata-only, snowplow 1.12.54 prewarms only identities a real requester can hit, and alert-provider 0.2.53 fixes root-cause analysis on deleted objects.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

core-provider 2.13.27 · Oct 23

- CDC watches CRDs with a metadata-only informer; a failed upgrade returns an error, not a panic.

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

snowplow 1.12.54 · Oct 23

- Prewarm seeds only reachable identities; RESTAction YAML conversion memoised.

github.com/krateo-platformops/snowplow/releases

installer 0.3.452 · Oct 23

- Pins core-provider 2.13.27, snowplow 1.12.54, incident-controller 0.5.0.

github.com/krateo-platformops/installer/releases

alert-provider 0.2.53 · Oct 23

- RCA handles full resource names and deleted objects.

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

observability 3.1.23 · Oct 23

- Collector-deployment 0.3.11 drops two replicaset gauges.

github.com/krateo-platformops/observability/releases

Latest elsewhere: portal 1.8.84 (Oct 22), frontend 1.8.10 (Oct 22), oasgen-provider 0.32.0 (Oct 19), helm-render-service 0.5.0 (Sep 30).

KRATEO AGENTIKO

Merged into main this week

Krateo Agentiko notifications could not be read this morning.

NEWS IN BRIEF

CERTIFICATES

cert-manager 1.21.3 stops copying a private key from a Secret the Certificate does not own

Released October 23, it also fixes an ACME ARI renewal loop, quotes Helm proxy values and moves to Go 1.26.10. The maintainers say all users should upgrade.

— cert-manager releases on GitHub
github.com/cert-manager/cert-manager/releases

OPEN SOURCE SECURITY

Anthropic's scanner mails maintainers unreviewed bug reports with patches

InfoQ, October 23 (launched October 8): over six months the models flagged 29,000+ candidates and humans triaged about 6,000. In Anthropic's own sample, 85 of 97 critical and high findings across 48 projects met its disclosure criteria. Projects opt in by pull request; some saw inflated severities.

— InfoQ
www.infoq.com/news/2026/10/anthropic-oss-security-scanner

NUMBER OF THE DAY

127,000 Requests at Symantec's AI honeypot *(Symantec, via Daily CyberSecurity)*

SIEM

Horizon3 publishes a working exploit for the FortiSIEM gRPC path traversal

CVE-2026-106173 hits FortiSIEM 7.0 to 7.5.0 and was patched October 13 (FG-IR-26-180); reports give 9.4 or 9.8. Not in KEV yet. Upgrade and block TCP 27918.

— Daily CyberSecurity, October 23
securityonline.info/fortisiem-vulnerability-cve-2026-106173-poc

OPENSTACK

Manila let other projects change a public share's access rules

OSSA-2026-046, October 20 (CVE-2026-71195): non-owners could also soft-delete or back up a foreign public share and edit export-location metadata by UUID. Fixed in 20.0.3, 21.0.3 and 22.0.2; 23.0.0 needs the Hibiscus patch.

— OpenStack security advisories
security.openstack.org/ossa/OSSA-2026-046.html

DEVELOPER PORTALS

Backstage 1.56.2 fixes installs broken by @yarnpkg/core 4.9.2

Released October 22, it makes the Yarn CLI module's @yarnpkg dependencies optional peers. 1.56.1 and 1.54.10, out October 21, match catalog URL locations in canonical form.

— Backstage releases on GitHub
github.com/backstage/backstage/releases

SERVERLESS

Lambda Web Functions serve many requests from one warm environment

InfoQ, October 23: Node.js only, five regions at launch, billed on active CPU plus memory for the environment's life. Custom domains and WAF need CloudFront in front; existing functions become Event Functions.

— InfoQ
www.infoq.com/news/2026/10/aws-lambda-web-functions

AUTOSCALING

Karpenter 1.14.3 moves to Go 1.26.10 and x/net 0.60.0

Released October 23 with 1.15.1, whose notes list only cherry-picks. 1.15.0 (October 10) added DRA prioritized alternatives and node repair as a voluntary disruption.

— Karpenter releases on GitHub
github.com/kubernetes-sigs/karpenter/releases

KUBECTL TIP

`kubectl uncordon my-node`

Make a node schedulable again *(kubernetes.io)*

PUZZLE · WORD SEARCH

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

FIND **BACKSTAGE · FORTISIEM · HAMI · IRONIC · KAMAJI · KARPENTER · KYVERNO · MANILA · PHP · SKYNET**

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

Words run in every direction, also backwards.



SOLUTION