All the cloud native news that's fit to reconcile

# The Daily Reconcile.

COUNTDOWN
2 days
to the OSC Kolkata CFP

VOL. I · NO. 307 TUESDAY, NOVEMBER 3, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ GITOPS
**Argo CD 3.5.7, 3.4.13 and 3.3.19 fix sync-window and log-stream bugs** P.2

◆ EXPLOITED
**Node-RED instances without adminAuth are being taken over, at 10.0** P.2

◆ LLM PLANS
**Anthropic renames Max 20x to Claude Ultra and drops its five-hour cap** P.2

KUBERNETES SECURITY

## Rancher's meta proxy handed users' own credentials to cloud provider APIs

*CVE-2026-88811 needs only a signed-in user opening a provisioning form. SUSE fixed it and two related flaws on October 29 in 2.15.3, 2.14.7, 2.13.11, 2.12.15 and 2.11.19.*

COMPILED FROM GITHUB ADVISORY GHSA-X82X-2QJ6-5RM2, OCTOBER 29; DAILY CYBERSECURITY, NOVEMBER 3

The meta proxy lets the Rancher UI query cloud APIs while provisioning. The advisory says it "did not consistently remove the caller's own Rancher credentials from the outgoing request", so session cookies and API tokens reached endpoints such as Amazon EC2 or DigitalOcean.

Sources disagree on severity: GitHub rates it 8.8 (CVSS v4, High), Daily CyberSecurity 9.1 (CVSS v3, critical). The releases also fix an SSRF, CVE-2026-88809 (7.6), and CVE-2026-104623 (6.3), which let any logged-in user start a shell pod in cattle-system. No exploitation is reported.

What to do: upgrade, rotate long-lived API tokens used with the proxy, invalidate sessions

*Continued on page 2*

### RANCHER, OCTOBER 29

**5** RELEASE LINES PATCHED

**4** PROVIDER FORMS NAMED

**3** FLAWS FIXED TOGETHER

**5** BACKPORT PULL REQUESTS

*GitHub advisory GHSA-x82x-2qj6-5rm2 and Daily CyberSecurity, November 3.*

AI INFERENCE

## vLLM 0.33 drops CUDA 12.9 and more than doubles a DeepSeek benchmark

*Released November 2 with 927 commits from 389 contributors, it moves to PyTorch 2.14.0 and ships CUDA 13.0 wheels and images only.*

COMPILED FROM GITHUB, VLLM-PROJECT/VLLM V0.33.0, NOVEMBER 2

In one pull request's benchmark, DeepSeek-V4.1-Flash with DSpark on GB300 rose from 1,373 to 3,390 output tokens per second. FlashInfer prefill cuts mean time to first token by 39-48% at 100k input on eight B200s.

Breaking changes: Medusa, the MLP speculator and the legacy Ray compiled-graph executor are gone, the NIXL connector needs NIXL 1.5 or newer, and requests sent while generation is paused get HTTP 503. Check base images before upgrading.

*Full story → github.com/vllm-project/vllm/releases/tag/v0.33.0*

PLATFORM ENGINEERING

## Uber puts 800+ MCP servers and 5,000 tools behind one gateway

*A crawler turns Protobuf and Thrift schemas into MCP tools.*

COMPILED FROM INFOQ, NOVEMBER 2

New tools stay disabled until their owning team enables them, and responses can be redacted for personal data. Uber gives no latency or cost figures.

*Full story → www.infoq.com/news/2026/11/uber-mcp-gateway-ai-agents*

CLOUD SECURITY

## Shopify finds open GKE Ingresses from inventory, not repos

*Inconclusive verdicts fell about 80%.*

COMPILED FROM INFOQ, NOVEMBER 2

Overexposed reads Cloud Asset Inventory, then sends one anonymous request per endpoint. "The repository shows intent; the cluster shows what is enforced."

*Full story → www.infoq.com/news/2026/11/shopify-kubernetes-ingresses*

AI TRAINING

## TorchTPU runs PyTorch on TPUs by swapping cuda for tpu

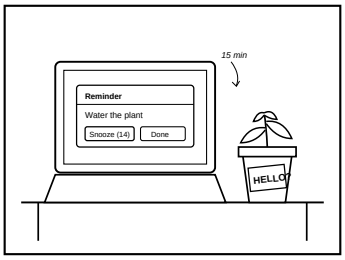
*Google and Meta's backend is early-stage.*

COMPILED FROM INFOQ, NOVEMBER 2

Google tested about 5,000 Hugging Face models; no licence or GA date is given.

*Full story → www.infoq.com/news/2026/11/torchtpu-native-pythorch-tpu*

### CARTOON OF THE DAY




*Drawing: Claude*

***The plant has started sending its own reminders.***

**WHY IT'S FUNNY** A laptop reminder to water the plant has been snoozed fourteen times, fifteen minutes at a time. The drooping plant has given up on the calendar and stuck a note of its own on the pot.

### DATES TO WATCH

*Events and calls for papers*

**Nov 5** CFP
Open Source Conference Kolkata (Dec 5): talks due

**Nov 9–12** EVENT
KubeCon + CloudNativeCon NA, Salt Lake City

**Nov 9** EVENT
Linkerd documentary premiere, KubeCon NA, Salt Palace room 151, 6:30 pm MST

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

# core-provider stops taking over Namespaces as eight components ship

**November 3, 2026 —** Eight components shipped on November 1 and 2: core-provider stops taking Namespace ownership, frontend and snowplow add table export, and Showback joins the installer.

KRATEO PLATFORMOPS

*GitHub releases, github.com/krateo-platformops*

**core-provider 2.13.51–2.13.54** · Nov 1

- Never takes Namespace ownership from another manager.

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

**snowplow 1.12.61–1.12.64** · Nov 1

- Step-up requests use the step-up credential; POST /export.

*github.com/krateo-platformops/snowplow/releases*

**frontend 1.8.17–1.8.18** · Nov 1-2

- Tables export to CSV, JSON or PDF; js-yaml CVE fixed.

*github.com/krateo-platformops/frontend/releases*

**oasgen-provider 0.47.0–0.49.0** · Nov 1-2

- Path-level parameters honoured; installer pins 0.48.0.

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

**installer 0.3.486–0.3.489** · Nov 1-2

- Showback becomes an installer component.

*github.com/krateo-platformops/installer/releases*

**authn, sse-proxy 0.31.1, 1.3.0** · Nov 1

- Expired step-up credentials purged; new /audit endpoint.

*github.com/krateo-platformops/authn/releases*

**alert-provider, observability 0.2.56–0.2.57, 3.1.30** · Nov 1-2

- Alerts reconciled in every namespace.

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

Latest elsewhere: provider-runtime 1.7.2 (Oct 31), portal 1.8.87 (Oct 29), helm-render-service 0.5.0 (Sep 30).

KRATEO AGENTIKO

*Merged into main this week*

No new Krateo Agentiko pull requests since the last issue.

CONTINUED FROM PAGE 1 · KUBERNETES SECURITY

## Rancher proxy

and look for unknown shell pods in cattle-system. There is no complete workaround.

*Full story → github.com/rancher/rancher/security/advisories/GHSA-x82x-2qj6-5rm2 securityonline.info/rancher-security-vulnerabilities-cve-2026-88811*

NEWS IN BRIEF

GITOPS

### Argo CD 3.5.7, 3.4.13 and 3.3.19 fix sync-window and log-stream bugs

The November 2 patches let sync-window-blocked operations terminate and plug a PodLogs goroutine leak. The gRPC health check no longer needs authentication. No CVEs are listed.

*— GitHub, argoproj/argo-cd, November 2*
*github.com/argoproj/argo-cd/releases*

NETWORKING

### Gateway API 1.7.0 is final, and HTTPRoute retries move to Standard

Released October 29, it graduates retry codes and attempts (GEP-1731) to the Standard channel. Experimental adds XTelemetryPolicy for tracing.

*— GitHub, kubernetes-sigs/gateway-api, October 29*
*github.com/kubernetes-sigs/gateway-api/releases*

NUMBER OF THE DAY

**3,390** vLLM output tok/s, up from 1,373 *(vLLM)*

EXPLOITED

### Node-RED instances without adminAuth are being taken over, at 10.0

VulnCheck says attacks on CVE-2026-58115 began October 30; over 20,000 admin interfaces are exposed. Enable adminAuth and keep port 1880 off the internet.

*— Daily CyberSecurity, November 3*
*securityonline.info/node-red-rce-vulnerability-cve-2026-58115*

LINUX

### 129 kernel CVEs in one week, two of them 9.8 in iSCSI

CVE-2026-99153 and CVE-2026-99154 let a malicious iSCSI target corrupt host memory. Fixed in 6.12.115, 6.18.59, 7.2.13 and other stable kernels.

*— Daily CyberSecurity, November 3*
*securityonline.info/linux-kernel-vulnerabilities-oct-26-nov-1-2026*

APACHE

### Apache fixes eight flaws in Fineract, Syncope and Arrow

Fineract 1.16.1 closes a 9.8 SQL injection; the article and advisory disagree on whether it needs a login. Syncope needs 4.0.9 or 4.1.4.

*— Daily CyberSecurity, November 3*
*securityonline.info/apache-security-vulnerabilities-syncope-fineract*

KUBECTL TIP

```
kubectl auth can-i --list
```

Everything you may do here *(kubernetes.io)*

LLM PLANS

### Anthropic renames Max 20x to Claude Ultra and drops its five-hour cap

Prices stay at $100 and $200 a month. The cap lifts only for accounts Anthropic verifies; the report cites a post on X.

*— Daily CyberSecurity, November 2*
*securityonline.info/claude-ultra-subscription-tier*

LLM PLANS

### OpenAI will pool ChatGPT and Codex usage from December

Plus, Pro and Business get one token-based quota; Instant chats are exempt.

*— Daily CyberSecurity, November 2*
*securityonline.info/chatgpt-codex-usage-limits*

WEB

### A robots.txt token lets sites opt out of AI training

Rules under User-Agent: __usage_ai-training do not block search indexing. Microsoft honours them from February 1, 2027, Google plans to in early 2027 and OpenAI over the coming months; Anthropic already does. Keep classic Disallow rules to shut crawlers out entirely.

*— Daily CyberSecurity, November 2*
*securityonline.info/ai-training-preference-standard*

KUBECTL TIP

```
kubectl api-resources -o wide
```

API resources with their verbs *(kubernetes.io)*

PUZZLE · WORD SEARCH

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

FIND ARGOCD · CREDENTIALS · GATEWAY · METAPROXY · NODERED · OVEREXPOSED · RANCHER · SYNCOPE · TORCHTPU · VLLM

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

*Words run in every direction, also backwards.*



SOLUTION