All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
14 days
to the Big Data Europe CFP

VOL. I · NO. 313 MONDAY, NOVEMBER 9, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ WAF SECURITY
ModSecurity's upload-rule bypass now has a public exploit; 3.0.17 fixes it P.2

◆ SUPPLY CHAIN
A translation file could inject code into uutils coreutils builds, rated 9.9 P.2

◆ NEW LLMS
Cognition's SWE-2 Flash is free until November 30, but its weights stay private P.2

AI CODING SECURITY

Claude Code's saved permissions leaked 2,539 secrets into 1,994 public repos

Answering "don't ask again" writes the whole command, password included, to a config file that often gets committed. The count is Apiiro's; Apiiro sells security tools.

COMPILED FROM DAILY CYBERSECURITY, NOVEMBER 8, CITING APIIRO RESEARCH

Apiiro researchers scanned 104,185 public copies of Claude Code config files on GitHub from November 1 to 3. Picking "Yes, and don't ask again" saves the exact command, secret included, to .claude/settings.local.json.

They found 398 service API tokens, 379 database passwords, 149 AI model API keys and 43 SSH logins. Gitleaks and TruffleHog missed 215 of the 1,122 exposed files, and 211 public forks hold copies.

Claude Code lead Boris Cherny said on November 7 the team is looking into it; no fix yet. What to do: find these files, rotate first, then untrack them and add agent folders to .gitignore.

Full story → securityonline.info/claude-code-leaking-secrets-github

APIIRO'S SCAN, BY THE NUMBERS

63	ORGANISATIONS NOTIFIED
43	SSH LOGINS EXPOSED
19	EXPOSED FILES SCANNERS MISSED, %
3	DAYS OF SCANNING, NOV 1-3

Apiiro scanned 104,185 public files; 215 of 1,122 exposed files evaded Gitleaks and TruffleHog.

AI SECURITY

A public exploit hits Hugging Face datasets 5.1.0, and no fixed release exists yet

CVE-2026-57845, rated 8.8, runs attacker code through the pandas builder's pickle loading. The library is downloaded about 38.4 million times a month.

COMPILED FROM DAILY CYBERSECURITY, NOVEMBER 9

The flaw sits in datasets.packaged_modules.pandas, which hands data files to pandas.read_pickle. Researcher Sai Teja Erukude found it and published the proof of concept; VulnCheck assigned the CVE on October 23 and rates it 8.7 under CVSS 4.0. Version 5.1.0, out October 5, and every earlier release are affected.

There is no fixed release. Pull request #8879 would make the pandas builder fail before it opens any file. No exploitation has been seen, and EPSS puts the 30-day chance at 0.5%.

What to do: never load untrusted datasets through the pandas builder. Use the Parquet, Arrow, CSV or JSON builders, or Dataset.from_pandas() instead of pickle files, and load third-party data in isolated, low-privilege Pods or jobs.

Full story → securityonline.info/hugging-face-datasets-rce-cve-2026-57845-poc

DEVELOPER PLATFORMS

Lima 2.3 runs VMs on Windows without QEMU

COMPILED FROM CNCF BLOG, NOVEMBER 8

Released November 6, the CNCF Incubating project adds an experimental hcs driver on WSL2's Host Compute System, one instance at a time. Linux gets real-IP networking via a sudoers helper.

Full story → www.cncf.io/blog/2026/11/08/lima-v2-3-native-on-windows-vmnet-on-linux-and-menu-tui

API SECURITY

IBM fixes 208 flaws in API Connect, three rated 9.9

COMPILED FROM DAILY CYBERSECURITY, NOVEMBER 9

Versions 10.0.8.0–10.0.8.12 and 12.1.0.0–12.1.1.2 are affected; the 9.9s include command injection and an LDAP injection reaching other tenants' admin. The report's summary box says nine CVEs. Apply bulletin 7295637.

Full story → securityonline.info/ibm-api-connect-vulnerabilities

SELF-HOSTED TOOLS

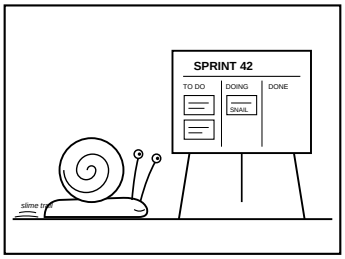
Penpot 2.18.0 closes a 9.9 file takeover

COMPILED FROM DAILY CYBERSECURITY, NOVEMBER 7

An import call skipped access checks, so any user could overwrite a file by its UUID; open sign-ups make it 10.0. Installs from version 1.20 on are affected, and a proof of concept is public. Until you upgrade, turn sign-ups off and check logs for odd project-id changes.

Full story → securityonline.info/penpot-file-takeover-ghsa-8qqw-wm58-45v7-poc-disclosed

CARTOON OF THE DAY



Drawing: Claude

"Good news: I've been assigned to the sprint."

WHY IT'S FUNNY A snail stands proudly in front of a Kanban board where its name sits in the "Doing" column of Sprint 42. A sprint is supposed to be a short burst of fast work, and nobody could be a worse fit for it, or prouder of the slime trail behind it.

DATES TO WATCH
Events and calls for papers

Nov 9 — EVENT
Platform Engineering Day, ArgoCon, BackstageCon and FluxCon NA, Salt Lake City

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

Nov 10 — ONLINE
Kubernetes monthly patch releases, target date

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

authn 0.37.0 lets a service act for a signed-in user

November 9, 2026 — On November 8, authn added delegated tokens and dropped per-user RESTAction copies, snowplow 1.12.67 put source IPs into audit events, and alert-provider 0.2.64 added per-group metric alerts.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

authn 0.37.0–0.38.0 · Nov 8

- A service can act for a signed-in person; the token names both.
- 0.38.0: RESTActions must read the token as ${ .token }; needs snowplow 1.12.28+.

github.com/krateo-platformops/authn/releases

snowplow 1.12.66–1.12.67 · Nov 8

- Audit events carry source IPs, User-Agent and URI.
- A pod is Ready only once the RBAC snapshot is complete.

github.com/krateo-platformops/snowplow/releases

alert-provider 0.2.64 · Nov 8

- Per-group metric alerts (groupBy, consecutiveWindows).

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

GitHub timed out on the other release pages this morning. Last reported: core-provider 2.13.75, installer 0.3.528, oasgen-provider 0.54.1 (Nov 7); plumbing has no releases.

KRATEO AGENTIKO

Merged into main this week

Krateo Agentiko notifications could not be read this morning.

NEWS IN BRIEF

WAF SECURITY

ModSecurity's upload-rule bypass now has a public exploit; 3.0.17 fixes it

CVE-2026-104269 (8.6) lets an RFC 2231 filename* header slip uploads past OWASP CRS rules in libmodsecurity 3.0.0 to 3.0.16. The fix shipped September 29; the proof of concept is new. Upgrade.

— Daily CyberSecurity, November 9
securityonline.info/modsecurity-vulnerabilities-poc

SUPPLY CHAIN

A translation file could inject code into uutils coreutils builds, rated 9.9

Under GHSA-c522-hqhp-v2qq, unescaped Fluent text in the uucore build script could inject Rust code. uucore 0.12.0 fixed it on September 17; a proof of concept followed November 9. Rebuild from a fixed tree.

— Daily CyberSecurity, November 9
securityonline.info/uutils-coreutils-vulnerability-poc

KERNEL SECURITY

Veeam now ships kernel fixes for the 9.8 TCP flaw, and Kasten is unaffected

Appliance 13.1 gets a fixed kernel for CVE-2026-98432 through Veeam Updater; Backup & Replication 13.1.2.57 on Windows needs a private fix, and 12.3's is coming. Kasten images carry no kernel.

— Daily CyberSecurity, November 6
securityonline.info/veeam-software-appliance-cve-2026-98432-patched

NEW LLMS

Cognition's SWE-2 Flash is free until November 30, but its weights stay private

Released November 4 in Devin, it is trained on Thinking Machines' open Inkling-Small (276B parameters, 12B active). Cognition claims one-fifth of SWE-2's price and 3x its speed, with no per-token price; its benchmark scores are its own.

— Let's Data Science, November 5; The New Stack, November 6
letsdatascience.com/blog/cognition-swe-2-flash-built-on-open-weights-wont-share-own

VULNERABILITY TRENDS

3,570 new CVEs in a week, and seven exploited ones are not in KEV

Daily CyberSecurity's count for November 2 to 8 has 311 critical and 1,220 high. Exploited flaws missing from CISA's catalog include Zyxel GS1900 switches and Sogou Input Method. Do not wait for KEV.

— Daily CyberSecurity, November 9
securityonline.info/weekly-cve-report-nov-2-8-2026

SERVERLESS DATA

Cloudflare's D1 control plane absorbs 18-fold growth in daily active databases

Postgres holds transactional metadata, ClickHouse analytics and Workers KV routing, with 30-second heartbeats jittered per database. Beyond the free tier, storage costs $0.75 per GB-month. The design is as Cloudflare describes it.

— InfoQ, November 8
www.infoq.com/news/2026/11/cloudflare-d1-control-plane

AI INFRASTRUCTURE

A CNCF paper lists the infrastructure gaps AI workloads hit

Published November 6, it covers topology awareness, GPU sharing, I/O bottlenecks and fault tolerance, and argues expensive GPUs should be shared when possible. It gives no figures.

— CNCF reports, November 6
www.cncf.io/reports/resource-and-infrastructure-challenges-for-ai-workloads

KUBECTL TIP

`kubectl config current-context`

Display the current context *(kubernetes.io)*

DEVELOPER TOOLS

Thomas Dohmke's Entire opens a Git forge built for coding agents

Review agents in a cloud sandbox score each push for quality, security and "slop". Entire claims pushes up to 89 times faster than GitHub; the figure is its own.

— InfoQ, November 8
www.infoq.com/news/2026/11/entire-git-forge-coding-agents

KUBECTL TIP

`kubectl get pods --all-namespaces`

List all pods in all namespaces *(kubernetes.io)*

NUMBER OF THE DAY

2,539 secrets leaked via Claude Code configs *(Apiiro, via Daily CyberSecurity)*

PUZZLE · WORD SEARCH

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

FIND COREUTILS · DATASETS · GITIGNORE · HEARTBEAT · LIMA · MODSECURITY · PENPOT · PICKLE · ROTATE · SECRETS

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

Words run in every direction, also backwards.

SOLUTION

