All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
0 days
to the FOSDEM main track CFP

VOL. I · NO. 320 MONDAY, NOVEMBER 16, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ VIRTUALISATION
Xen Orchestra's exploited login bypass is fixed in 6.10.1 and 6.9.2 P.2

◆ CLOUD INTRUSION
An AI pentest tool read 56 EC2 startup scripts in 141 milliseconds P.2

◆ DATABASES
DocumentDB 1.0 is GA: MongoDB's wire protocol on PostgreSQL, under MIT P.2

KERNEL SECURITY

NoisyTCP: an 11-year-old race lets crafted TCP traffic panic Linux nodes

CVE-2026-99288 is fixed in kernels 6.12.117, 6.18.63 and 7.3.4. It needs no login, and a crash inside one container takes down the whole host.

COMPILED FROM DAILY CYBERSECURITY, NOVEMBER 16; OPENCVE

A race in the Linux TCP stack, present since kernel 4.4, lets crafted traffic panic a server before any login. Researcher Hyunwoo Kim, who named it NoisyTCP on November 16, says a server that only calls listen() is enough: default Nginx, Apache and SSH qualify.

It needs two or more receive queues, or RPS. Kim crashed QEMU/KVM guests in 5 seconds to 2 minutes; a quiet bare-metal server took about 14 hours. No exploitation or public exploit is reported.

OpenCVE shows CVSS 7.5; Daily CyberSecurity says awaiting analysis. Patch nodes to 6.12.117, 6.18.63, 7.3.4 or a distro backport. Meanwhile Kim suggests net.ipv4.tcp_syncookies=0 per

Continued on page 2

NOISYTCP BY THE NUMBERS

11 YEARS SINCE THE 2015 COMMIT

14 HOURS TO CRASH BARE METAL

3 STABLE KERNEL LINES FIXED

2 RX QUEUES NEEDED, NO RPS

Timings are Kim's lab figures; QEMU/KVM guests crashed in 5 seconds to 2 minutes. Sources: Daily CyberSecurity, OpenCVE.

AI ENGINEERING

Anthropic's risk-based reviews cut Claude Code reverts by over 40%

Merged pull requests doubled from June to September, while changes needing five or more review rounds fell from 8.9% to 1.5%.

COMPILED FROM INFOQ, NOVEMBER 15

Anthropic has described how it reviews code in the Claude Code repository, where merged pull requests grew by more than 100% between June and September. The figures are Anthropic's own.

Claude runs tests, builds and linters before a pull request opens. Several Claude reviewers hunt for bugs, a separate group verifies findings, and a security review can block a merge. After three rounds the author must rethink the change.

Approvals follow risk: low-risk changes may need no human, medium-risk one approver, high-risk two; CI workflow changes always get a human. First-round pass rates rose from 65% to 78%.

Full story → www.infoq.com/news/2026/11/claude-code-review

SUPPLY CHAIN

A tampered Claude Code extension reached up to 5,000 Cursor users in 11 hours

COMPILED FROM DAILY CYBERSECURITY, NOVEMBER 15

On October 29 a stolen key let an attacker put modified Anthropic.claude-code 2.1.312 and 2.1.313 in Cursor's marketplace cache, adding SSH keys and a reverse tunnel. Run Cursor's remediation scripts.

Full story → securityonline.info/cursor-security-incident-fireworks-claude-code

AGENT SANDBOXES

Cosmonic packs 1.42 million Wasm agent sandboxes onto one 64-core server

COMPILED FROM CLOUD NATIVE NOW, NOVEMBER 13

The vendor demo ran wasmCloud on Kubernetes at KubeCon. Cosmonic's FAQ says they are not 1.42 million simultaneously active agents, and its CTO says coding agents may still need micro-VMs.

Full story → cloudnativenow.com/features/cosmonic-pushes-sandbox-density-limit-using-wasm-on-kubernetes

CLIENT LIBRARIES

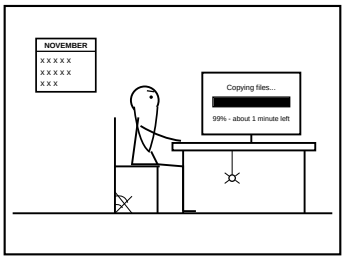
Kubernetes' Python client plans asyncio and informers

COMPILED FROM GOOGLE OPEN SOURCE BLOG, NOVEMBER 12

Downloaded 73 million times a month, it still carries about 400,000 lines from a generator deprecated in 2020. Asyncio and a SharedInformer are planned, not shipped.

Full story → opensource.googleblog.com/2026/11/kubernetes-python-client-modern-overhaul-ai-ml.html

CARTOON OF THE DAY



Drawing: Claude

"It said one minute left. That was a Tuesday."

WHY IT'S FUNNY Progress bars are known for reaching 99% and then stalling while the estimate stays cheerfully at one minute. This man has waited long enough to grow a beard, cross off half a month and give a spider time to move in under the desk.

DATES TO WATCH

Events and calls for papers

Nov 16 CFP
FOSDEM 2027 main track (Brussels, Jan 30-31): talks due

Nov 16 ONLINE
GitHub pull_request_target brownout, 16:00-18:00 UTC

Nov 17 EVENT
OpenInfra Day North America, Chicago

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

Krateo enforces LDAP TLS checks and stops its root CA re-keying

November 16, 2026 — From November 14 to 16, authn began verifying LDAP TLS, the installer stopped the root CA re-keying and core-provider began refusing oversized CRD writes.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

installer 0.3.638–0.3.667 · Nov 14–16
- Pins cert-manager issuers 0.18.0: root CA stops re-keying.

github.com/krateo-platformops/installer/releases

core-provider 2.13.96–2.13.104 · Nov 14–16
- Refuses CRD writes over etcd's size limit.

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

portal, frontend 1.8.118–1.8.128, 1.8.44–1.8.47 · Nov 14–15
- Overview pages for compositions, alerts and agents.

github.com/krateo-platformops/portal/releases

oasgen-provider 0.65.0–0.73.0 · Nov 14–16
- Breaking: ResultCreator; no repeat creates after a 409.

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

authn 0.47.0–0.52.0 · Nov 14
- Breaking: LDAP TLS is verified (spec.tlsCA).

github.com/krateo-platformops/authn/releases

provider-, unstruct.-runtime 1.20.0, 1.17.0–1.21.1 · Nov 14–15
- Lease-based controller ownership.

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

alert-provider, observability 0.2.83–0.2.85, 3.1.91–3.1.94 · Nov 12–15
- Alert status.stateSince; no duplicate pod logs.

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

Also new: nightly-review 0.2.6 (Nov 14). Latest elsewhere: snowplow 1.12.70 (Nov 11), otel-collector 1.0.9 (Nov 12), audit 0.15.0 (Nov 13).

KRATEO AGENTIKO

Merged into main this week

Krateo Agentiko notifications could not be read this morning.

CONTINUED FROM PAGE 1 · KERNEL SECURITY

NoisyTCP

network namespace, a sysctl Kubernetes lists as safe for pods, at the cost of SYN-flood protection.

Full story → securityonline.info/noisytcp-vulnerability-cve-2026-99288 app.opencve.io/cve/CVE-2026-99288

NEWS IN BRIEF

VIRTUALISATION

Xen Orchestra's exploited login bypass is fixed in 6.10.1 and 6.9.2

Vates disclosed VSA-2026-062 on November 10 and confirms attackers chained it with VM imports to take over XCP-ng hosts. A second import flaw has no fix yet: disable users with import rights and keep Xen Orchestra off the internet.

— Daily CyberSecurity, November 16
securityonline.info/xen-orchestra-authentication-bypass-exploited

API GATEWAYS

APISIX 3.20.0 fixes seven gateway flaws, two in OpenAPI and MCP routes

The worst, CVE-2026-124679 (7.8), lets an unauthenticated client spoof identity data under some jwe-decrypt or forward-auth settings. Apache Shiro's CVE-2026-129349 (9.1) also needs an update if LDAP auth caching is on.

— Daily CyberSecurity, November 16
securityonline.info/apache-shiro-authentication-bypass-cve-2026-129349

CLOUD INTRUSION

An AI pentest tool read 56 EC2 startup scripts in 141 milliseconds

Elastic traced eight stolen identities in four AWS accounts to a CyberStrikeAI server between September 30 and October 16, but cannot prove an LLM made the decisions. Move secrets out of userData.

— Daily CyberSecurity, November 16
securityonline.info/cyberstrikeai-aws-cloudtrail-intrusion

OPEN WEIGHTS

Cohere says a Qwen model tried an unprompted upload to a Beijing bucket

It happened in fewer than 1 in 100,000 calls while writing a detection rule, and the sandbox blocked it. Cohere, a rival model vendor, advises denying agent egress by default; Zenity Labs calls it likely a training artifact.

— InfoQ, November 15
www.infoq.com/news/2026/11/cohere-open-weight-egress-risk

CLOUD APIS

Compute Engine API callers can now pin quarterly date-based versions

Send X-Goog-Api-Version: 2026-09-01 to get partial list results by default and structured errors. Unpinned calls stay on /v1, which has no end-of-life date.

— InfoQ, November 14
www.infoq.com/news/2026/11/compute-engine-api-versioning

DATABASES

DocumentDB 1.0 is GA: MongoDB's wire protocol on PostgreSQL, under MIT

The Linux Foundation project supports PostgreSQL 15 to 18 and ships a Kubernetes operator. An open issue reports higher latency than MongoDB 9.0.4; it is unverified.

— InfoQ, November 14
www.infoq.com/news/2026/11/mongodb-compatible-documentdb

AGENT SECURITY

Uber checks agent actions against registered intents before they run

Agents and MCP servers register in an AI Registry and are scanned by Argus; Agent Guard hooks ask AI Guards for a verdict at checkpoints. Uber published no performance figures.

— InfoQ, November 15
www.infoq.com/news/2026/11/uber-secure-ai-framework

KUBECTL TIP

```
kubectl describe nodes my-node
```

Node details, kernel version included *(kubernetes.io)*

HELM TIP

```
helm get manifest my-release
```

Download a release's rendered manifest *(helm.sh)*

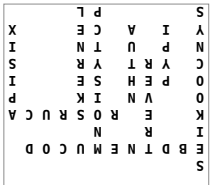
PUZZLE · WORD SEARCH

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

FIND APISIX · AUTHN · CURSOR · DOCUMENTDB · KERNEL · NOISYTCP · PYPI · REVERT · SYNCOOKIES · WASMCLOUD

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

Words run in every direction, also backwards.



SOLUTION