All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
0 days
to the GENAIX Singapore CFP

VOL. I · NO. 288 THURSDAY, OCTOBER 15, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ OBSERVABILITY
The OpenTelemetry Collector now refuses to start on a deprecated supervisor flag P.2

◆ SUPPLY CHAIN
An npm trust configuration that never publishes now expires after 48 hours P.2

◆ AI PLATFORMS
An LLM platform hands out admin tokens from an unauthenticated SSO endpoint P.2

CLOUD NATIVE SECURITY

Three 9.2 flaws in NGINX reach the ingress controller and Gateway Fabric

F5 published three advisories on October 14. All three are memory corruption, none needs a login, and the fix list runs to ten releases.

COMPILED FROM SECURITYONLINE.INFO, F5 ADVISORIES K000162608, K000162607 AND K000162416

CVE-2026-97205 is a use-after-free in ngx_http_core_module. CVE-2026-93479 is a heap buffer overflow in regex map handling, CVE-2026-15176 one in alias and rewrite handling. Each is scored 9.2 on CVSS v4.0, and each lets an unauthenticated attacker crash workers or run code.

NGINX Open Source 1.31.0–1.31.6 and 1.30.0–1.30.5 are affected, and NGINX Plus 37.0.0–37.0.4 and R33–R36. For cluster operators the names that matter are NGINX Ingress Controller and NGINX Gateway Fabric, both on the list with Instance Manager and F5 WAF for NGINX.

Go to 1.31.7 or 1.30.6, Plus 37.1.0.1, Ingress Controller 5.7.0, Gateway Fabric 2.8.0. Until then: aio off or ssi off, and no alias in location blocks.

Full story → securityonline.info/f5-patches-three-critical-nginx-vulnerabilities

WHAT F5 SHIPPED ON OCTOBER 14

3 FLAWS, ALL AT 9.2

7 PRODUCTS AFFECTED

10 FIXED RELEASES

3 WORKAROUNDS OFFERED

Three advisories, the F5 and NGINX products carrying the vulnerable code, the releases that carry the fix, and the stopgaps for teams that cannot patch today. Source: securityonline.info, F5.

AI AND HPC ON KUBERNETES

Before blaming the scheduler, ask whether Kueue admitted the workload at all

A Kubernetes blog walkthrough on October 14, with a read-only Headlamp plugin at 0.1.0-alpha.

COMPILED FROM KUBERNETES.IO, HEADLAMP.DEV

Admission and Pod scheduling are two decisions, and the post is blunt about the order: "The useful question is not only 'Why is the Pod pending?' It is first 'Has Kueue admitted the Workload?'" Admission weighs queue policy, quota, ResourceFlavors and the other Workloads waiting.

The example is a ClusterQueue with two CPUs and two Pod slots and a Job of three Pods asking one CPU each. Kueue reads the PodSets, not one Pod template, so the request is three CPUs and 600 MiB: the Workload is Inadmissible.

Full story → kubernetes.io/blog/2026/10/14/tracing-kueue-admission-with-headlamp github.com/headlamp-k8s/plugins/issues/1251

HPC ON KUBERNETES

Volcano 1.16.0 gives tenants queue hierarchies inside their own namespaces

Released October 14 by 65 contributors. Namespace queues go five levels deep and fair share decays over four hours.

COMPILED FROM GITHUB.COM/VOLCANO-SH/VOLCANO

NamespaceQueue, off by default, lets a tenant build queues and quotas inside a namespace, five levels below a cluster Queue unless --max-namespacequeue-depth says otherwise. The new fair-

Continued on page 2

CLOUD NATIVE SECURITY

A built-in Collabora server is dropping webshells on Nextcloud hosts

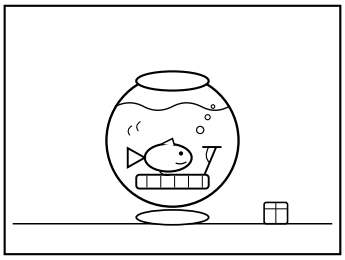
CVE-2026-110447, CVSS v4 9.2, exploited through September and October. Patching does not remove a backdoor already there.

COMPILED FROM SECURITYONLINE.INFO, NEXTCLOUD COMMUNITY ALERT

The flaw is in proxy.php in the richdocumentscode app, reached at /apps/richdocumentscode/proxy.php?status with encoded traversal, and it fires when the bundled CODE server is not running. Unescaped path input lands in the AppImage launch arguments, where $() and ${IFS} run as shell commands. Fixed in 26.4.303; standalone Collabora is not affected.

Full story → securityonline.info/nextcloud-collabora-online-cve-2026-110447-exploited

CARTOON OF THE DAY



Drawing: Claude

Leg day.

WHY IT'S FUNNY The goldfish has installed a treadmill at the bottom of its bowl, with a towel over the handrail. It spends every waking hour swimming already, and it has no legs. The joke is the fitness routine bolted onto a life that was nothing but exercise to begin with.

DATES TO WATCH

Events and calls for papers

Oct 15 ONLINE
KubeVirt Summit Virtual, 12:00–16:00 UTC, free; ten years of KubeVirt

Oct 15 CFP
GENAIX Global Generative and Agentic AI Summit (Singapore, Apr 16, 2027): talks due today

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

snowplow 1.12.47 closes two RBAC races, and the installer shipped it the same day

October 15, 2026 — Five components moved on October 14: snowplow to 1.12.47, core-provider to 2.13.25, the portal to 1.8.72, the frontend to 1.8.5 and the installer to 0.3.426.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

snowplow 1.12.47 · Oct 14

- Security: two RBAC race conditions could leave a revoked subject with access after a snapshot was published.

github.com/krateo-platformops/snowplow/releases

core-provider 2.13.25 · Oct 14

- Repairs composition-version policy mutation, broken since 2.13.23 because the charts still called the old method.

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

portal 1.8.72 · Oct 14

- Global search returned no blueprints: a duplicate filter key had silently dropped a projection.

github.com/krateo-platformops/portal/releases

Latest elsewhere: installer 0.3.426, frontend 1.8.5 and sse-proxy 1.1.9 (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 · HPC ON KUBERNETES

Volcano 1.16

share plugin tracks usage per namespace with a 240-minute half-life, and must sit before drf to count.

Full story → github.com/volcano-sh/volcano/releases/tag/v1.16.0

SUPPLY CHAIN

Working exploit code for the GitLab 10.0, and a count: 25,766 hosts

New on CVE-2026-97229, reported here October 13: Rapid7 published a proof-of-concept and Censys measured the exposure.

COMPILED FROM SECURITYONLINE.INFO, RAPID7, CENSYS

Censys finds about 25,766 internet-facing hosts on vulnerable releases, 31 per cent of the 82,454 GitLab hosts it detects. Exploitation is not confirmed and EPSS is 0.6 per cent. Self-managed 19.2.x, 19.3.x and 19.4.x need 19.2.8, 19.3.5 or 19.4.2.

Full story → securityonline.info/gitlab-rce-cve-2026-97229-poc-disclosed

NEWS IN BRIEF

OBSERVABILITY

The OpenTelemetry Collector now refuses to start on a deprecated supervisor flag

v1.2.0 / v0.163.0 landed on October 14. The supervisor now fails to start if reports_remote_config is still true; use accepts_remote_config. The sqlserver receiver is renamed sql_server, and SQL Server database counters gain a sqlserver.database.name attribute, splitting one series into one per database.

— github.com/open-telemetry/opentelemetry-collector-contrib
github.com/open-telemetry/opentelemetry-collector-contrib/releases/tag/v0.163.0

CLOUD NATIVE SECURITY

Palo Alto's management interface is being exploited for root, with no workaround

CVE-2026-0322, CVSS v4 8.6, carries the vendor's highest urgency rating, and the advisory says "very limited exploitation has been observed" against the management interface. An authenticated attacker with network access to it runs code as root. Fixes are 12.2.4, 11.2.16 and 10.2.18-h12; no workarounds exist.

— securityonline.info, Palo Alto Networks
securityonline.info/palo-alto-pan-os-rce-cve-2026-0322-exploited

SUPPLY CHAIN

An npm trust configuration that never publishes now expires after 48 hours

Covered on October 15; announced on October 2. Until its first publish, a trusted publishing configuration trusts the owner/repo and workflow file name, not the repository's immutable identity, so a renamed repository can be re-registered by somebody else. Researchers put over 1,500 packages in range.

— securityonline.info, GitHub
securityonline.info/npm-trusted-publishing

AI PLATFORMS

An LLM platform hands out admin tokens from an unauthenticated SSO endpoint

CERT/CC published VU#166125 on October 15. In DataElement Bisheng, POST /user/sso issues a valid JWT for any username when BISHENG_PRO is enabled: ask for the admin name and you are super-administrator. CVE-2026-96679 is scored 9.8 and unpatched. Disable the sso() function.

— securityonline.info, CERT/CC
securityonline.info/cert-cc-dataelement-bishe ng-vulnerabilities-sso

VIRTUALISATION

A grant-table race in XenServer lets a guest reach the host

Citrix shipped CTX697170 on October 15 for XenServer 8.4 and 9. Three of the four issues "may allow a malicious privileged user in a guest VM to compromise or crash the host": a grant-table version race, a stack overflow in tapdisk and a page reference leak. Restrict guests to grant table version 1 until patched.

— securityonline.info, Citrix, Xen Project
securityonline.info/citrix-security-update-xen server-uniconos

KUBECTL TIP

`kubectl describe workload -n dev`

Why Kueue has not admitted a job *(kubernetes.io)*

PUZZLE · WORD SEARCH

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

FIND COLLABORA · GITLAB · HEADLAMP · KUEUE · NGINX · SNOWPLOW · TRIVY · VOLCANO · WORKLOAD · XENSERVER

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

Words run in every direction, also backwards.

SOLUTION

