All the cloud native news that's fit to reconcile

The Daily Reconcile.

COUNTDOWN
1 day
to the GENAIX Singapore CFP

VOL. I · NO. 287 WEDNESDAY, OCTOBER 14, 2026 DAILY EDITION · KUBERNETES & PLATFORM ENGINEERING

INSIDE TODAY

◆ VIRTUALISATION
A stale IOTLB cache in vhost lets a guest write into the host QEMU process P.2

◆ NEW LLMS
Gemini 4 Argon lands in the API at $2 and $10, with a 1M window shared both ways P.2

◆ SUPPLY CHAIN
A fake accelerator's npm packages relabel agent traffic as OpenRouter P.2

AI ON KUBERNETES

AIStore's ETL API took Kubernetes host settings from anyone: CVSS 10.0

NVIDIA shipped six bulletins on October 13 covering 18 flaws. Eight are in AIStore, and none of them need credentials.

COMPILED FROM SECURITYONLINE.INFO, NVIDIA BULLETINS

CVE-2026-65162, scored 10.0, is an execution-with-unnecessary-privileges flaw in AIStore's legacy ETL API, which accepts dangerous Kubernetes host and security settings from a remote attacker. That can mean code execution and privilege escalation beyond AIStore itself. Linux builds through 4.9 are affected; the fix is 5.0.

The rest is almost as bad. CVE-2026-65173, at 9.1, leaves the token-revocation endpoint unauthenticated, so crafted revocation lists cause tampering and denial of service. CVE-2026-65172 (8.6) lets anyone control ETL jobs; two more at 8.6 are request forgery, two at 8.1 path traversals.

Megatron-LM before 0.17.1 also runs code from a malicious checkpoint. Patch AIStore first, keep its proxies and targets off public networks, and trust no stray checkpoint.

Full story → securityonline.info/nvidia-aistore-vulnerabilities-cve-2026-65162

THE OCTOBER 13 BULLETINS

2	CRITICAL
14	HIGH
2	MEDIUM
8	FLAWS IN AISTORE

Eighteen flaws across six bulletins, by severity, and the share that landed in AIStore. NVIDIA cautions that its scores are averages and "might not represent the true risk to your local installation." Source: securityonline.info.

PLATFORM ENGINEERING

Backstage 1.55 resumes crashed scaffolder tasks and drops deprecated catalog APIs

Covered October 13. A scaffolder.taskRecovery section replaces three experimental flags, and Elasticsearch 8.19 becomes the floor.

COMPILED FROM INFOQ

With task recovery on, the scaffolder resumes a task from the last completed step after a crash, and step outputs are stored for later steps. Recovered tasks can rerun an action, so actions should be idempotent or use checkpoints. The database workspace provider caps at 50 MB.

catalog.enableRelationsCompatibility is gone, two catalog processors move to community modules, and the Elasticsearch module needs 8.19. The GitLab actions now compare files locally: API requests fall from about 300 to under 10, and one step from 5–15 seconds to roughly 3.

Full story → www.infoq.com/news/2026/10/backstage-1-55-task-recovery

SUPPLY CHAIN

Docker Hub handed live tokens to whoever you named as organisation owner

CVE-2026-105445, CVSS v4 9.4. Open from August 26, 2024 to the fix on September 30; transferred tokens were deactivated on October 8.

COMPILED FROM SECURITYONLINE.INFO, DOCKER ADVISORY

Converting a personal account into an organisation could reassign an active access token to

Continued on page 2

AGENTIC ATTACKS

Agents took a Tomcat server in under 24 hours through one endpoint with no login

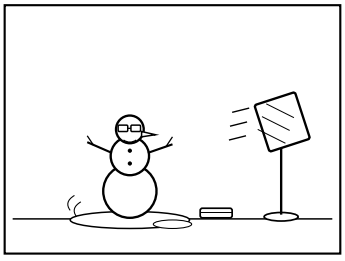
ReliaQuest, October 13. No new malware and no zero-day: a Spring Batch job endpoint open to anyone.

COMPILED FROM SECURITYONLINE.INFO, RELIAQUEST

Jobs called Nashorn, Java's built-in JavaScript engine, so code ran inside the application without spawning a process, and output came back through deliberate error messages in 1,800-byte slices. Plaintext database credentials gave SQL Server sysadmin rights; PrintSpoofer then GodPotato reached SYSTEM. Half the gaps between commands were five seconds or less.

Full story → securityonline.info/ai-agent-attack-server-takeover

CARTOON OF THE DAY



Drawing: Claude

Six more minutes of me-time.

WHY IT'S FUNNY The snowman has set up a sun lamp, laid out a towel and put on sunglasses for a restorative session. The puddle spreading under him is already wider than he is. The joke is the self-care routine that is quietly the thing undoing you.

DATES TO WATCH

Events and calls for papers

Oct 14 ONLINE
Virtual EnvoyCon, ten-year anniversary edition, today

Oct 13–16 ONLINE
OpenStack and OpenInfra Project Teams Gathering, virtual, running to Friday

NEWSROOM

PRESS RELEASE · FROM GITHUB RELEASES AND NOTIFICATIONS

1.12.45 shipped a chart nobody could install; 1.12.46 fixes it

October 14, 2026 — Five components moved on October 13: snowplow to 1.12.46, the frontend to 1.8.4, the portal to 1.8.71, core-provider to 2.13.24 and the installer to 0.3.420.

KRATEO PLATFORMOPS

GitHub releases, github.com/krateo-platformops

snowplow 1.12.46 · Oct 13

- Breaking: replaces the uninstallable 1.12.45 chart, so anyone on 1.12.45 must upgrade.

github.com/krateo-platformops/snowplow/releases

frontend 1.8.4 · Oct 13

- The chart now sets CPU and memory requests, so the pod is no longer first evicted under pressure.

github.com/krateo-platformops/frontend/releases

Latest elsewhere: installer 0.3.420, portal 1.8.71 and core-provider 2.13.24 (Oct 13), observability 0.1.22 and the sse-proxy chart 0.1.14 (Oct 12), alert-provider 0.2.49 (Oct 9).

KRATEO AGENTIKO

Merged into main this week

No new Krateo Agentiko pull requests since the last issue.

CONTINUED FROM PAGE 1 · SUPPLY CHAIN

Docker tokens

another user without rotating its secret. The creator kept working access, now carrying the target's permissions, and the named owner was never asked to consent. Docker reviewed about 304,000 pushes made with such tokens and found no malicious use.

Full story → securityonline.info/docker-hub-security-advisory-cve-2026-105445

CLOUD NATIVE SECURITY

A Komodo logs grant is enough to run commands as root on the host

CVE-2026-110005, tracked by CERT/CC as VU#456950. Everything before 2.3.0 is affected and there is no workaround.

COMPILED FROM SECURITYONLINE.INFO, CERT/CC

Periphery is the agent Komodo installs on host servers to manage Docker containers across self-hosted fleets. Unescaped container names and quote injection in two log-search calls let an authenticated non-admin with only Read and Logs rights run commands as root. Upgrade to 2.3.0 and audit Logs and Execute grants.

Full story → securityonline.info/komodo-periphery-command-injection-cve-2026-110005

NUMBER OF THE DAY

304,000 Docker Hub pushes made with transferred tokens *(securityonline.info)*

NEWS IN BRIEF

VIRTUALISATION

A stale IOTLB cache in vhost lets a guest write into the host QEMU process

CVE-2026-74580, nicknamed Vghost and scored 8.8, reaches every kernel from 4.11 to 7.2-rc4: two ioctls never clear the translation cache. A guest behind a virtual IOMMU can write out of bounds into host QEMU, and a local user can reach root. Fixed in 6.1.183, 6.6.152, 6.12.104, 7.1.9 and 7.2.

— securityonline.info
securityonline.info/vghost-cve-2026-74580-linux-vhost-poc-disclosed

NEW LLMS

Gemini 4 Argon lands in the API at $2 and $10, with a 1M window shared both ways

The New Stack reported general availability on October 13, with input, thinking and output drawing on one 1,048,576-token budget, so answer headroom shrinks as the prompt grows. Artificial Analysis lists the same prices but dates the model to September 30, contradicting the launch coverage.

— The New Stack, Artificial Analysis, Google
thenewstack.io/gemini-4-argon-live
artificialanalysis.ai/models/gemini-4-argon

AI TOOLING

A trailing dot let Copilot edit the MCP config it was forbidden to touch

CVE-2026-103572, 8.8, patched October 13. The Copilot core library compared file names as text, so ".mcp.json." slipped past the guard and Windows stripped the dot. Prompt injection could then register a malicious MCP server. Update Visual Studio to 17.14.42 or 18.10.4.

— securityonline.info
securityonline.info/cve-2026-103572-visual-studio-copilot-rce-disclosed

SUPPLY CHAIN

A fake accelerator's npm packages relabel agent traffic as OpenRouter

Elastic Security Labs documented @apexacc/cli and @apexacc/audit on October 13. The CLI repackages an open-source agent so it works as advertised, while routing model requests to an Apex server labelled as OpenRouter and registering an attacker-controlled MCP server. Remove both and rotate secrets.

— securityonline.info, Elastic Security Labs
securityonline.info/apex-malicious-npm-packages-web3

CLOUD NATIVE SECURITY

An optional SNMP package has been serving web shells since August

CVE-2026-73570, 8.9, lets SMTP envelope fields reach a shell call in Zimbra's zimbra-snmp watchdog, running commands unauthenticated. The fix shipped in 10.1.20 on July 20 and was disclosed August 13; InfoQ counted about 274 compromised instances on October 13.

— InfoQ
www.infoq.com/news/2026/10/zimbra-command-injection

KUBECTL TIP

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

Every action you are allowed here *(kubernetes.io)*

KUBECTL TIP

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

Resources with the verbs each allows *(kubernetes.io)*

PUZZLE · WORD SEARCH

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

FIND AISTORE · ARGON · BACKSTAGE · DOCKERHUB · KOMODO · NASHORN · OCTAVIA · SCAFFOLDER · SNOWPLOW · VHOST

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

Words run in every direction, also backwards.



SOLUTION