ISSUE 01 · WEEKLY · FREE TO SHARE · 24 – 30 OCT 2026

SECURITY WEEK IN REVIEW

CURATED BY IJAZ · ALL INDUSTRIES · FOR LEADERS AND TECH TEAMS

BREAKING

One laptop. $6.3 billion gone.

The biggest crypto theft on record didn't need a stolen key, just a trusted engineer's computer. What it means for any business that moves money or data.

ALSO INSIDE

- A hospital pulls the plug in 40 minutes
- Patched isn't the same as clean
- 750,000 people, no login needed
- Your weekend playlist

WELCOME

Welcome to Issue 01

A Friday read for anyone who makes security decisions, whether you sign off the budget or run the systems.

A lot happens in security every week, and most of it reaches us as scattered headlines. This is my attempt to pull the week together in one place, in plain English, with enough technical detail that tech teams still get something real out of it.

This first week ran from a crypto exchange to a US hospital to a national government, and one pattern links them all. My take on it is on the next page.

Read it in two minutes or twenty. Either way, tell me where you disagree.

Ijaz

PICK YOUR PACE

2 min
The 30-second briefing and my take, page 3

10 min
The week's stories, pages 4 to 9

Act
Your Monday checklist, page 13

Talk
Pick a side in the comments, page 14

START HERE

Your 30-second briefing

FINANCE & CRYPTO	About $6.3B was taken from Binance after one engineer's laptop was compromised.
HEALTHCARE	UNM Health, a US trauma centre, unplugged its computers within 40 minutes of a breach.
CRITICAL INFRASTRUCTURE	Hackers stole encryption keys from Cisco SD-WAN gear, and Volt Typhoon hit US utilities.
PUBLIC SECTOR	Attackers pulled data on 750,000 people from Moldova's government e-services.

IJAZ'S TAKE

The pattern for me this week: attackers went after things we trust to act on our behalf. An engineer's laptop, a network controller, a package update, a government lookup service. We spend a lot proving who someone is at login, and far less asking what our own systems will do once they trust something. That's the gap I'd look at first.

Ijaz · views my own, not my employer's

BREAKING STORY OF THE WEEK

CONFIRMED INCIDENT | FINANCE & CRYPTO | LOGINS & ACCESS

One laptop, $6.3 billion

The keys were safe. The system that asks for money wasn't.

AFFECTED Binance (crypto exchange) and its customers · 17 hot wallets · losses covered by Binance

FOR YOUR BUSINESS

One laptop should never be enough to move money.

WHAT HAPPENED

About $6.3B left Binance's **hot wallets** (crypto kept online for quick payouts). A DevOps engineer's laptop was used to reach a service container and push withdrawals. No private-key leak found.

↳ *Source: Euronews · TNGlobal · CoinDesk*

HOW IT UNFOLDED

- **Thu** Unauthorised withdrawals start draining hot wallets.
- **Fri** Theft stops after about 4 hours. Withdrawals frozen.
- **Fri** About $2.7B frozen. TRM Labs blames North Korea's TraderTraitor.
- **Fri** Binance will cover losses, with withdrawals back in ~45 hours.

BREAKING · CONTINUED

Why it matters, and what to do

Most security money goes into protecting keys. Far less goes into who, or what, may ask for a payment, and from which device.

Protecting the key is half the job. The other half is who can ask it to sign.

IF YOU LEAD A TEAM

Ask which systems can move money or data on their own, and whether a single laptop is enough to trigger them. Insist on a second, separate approval for large payouts.

IF YOU RUN THE TECH

No standing production access from engineer laptops: just-in-time elevation, privileged-access workstations, velocity limits and out-of-band multi-party approval on signing services.

WHAT IT MEANS HERE (GCC)

VARA-licensed exchanges and CBUAE-regulated payment firms run similar hot-wallet and automated-payout setups. Expect questions on who can approve a payout, and from which device.

QUESTIONS TO ASK YOUR TEAM OR PROVIDER

Can one laptop trigger a payment or data export? Who approves large automated payouts, and from where? How fast would we notice?

NEXT FRONTIER

Attackers are moving from stealing keys to abusing the automation around them: signing services, build pipelines, payment engines.

BY THE NUMBERS

The week in four figures

$6.3 bn

estimated taken from Binance's hot wallets in under four hours

↳ *Source: Euronews (Binance figures)*

40 min

from UNM Health spotting a breach to telling staff to unplug

↳ *Source: Help Net Security*

750k people

whose ID numbers were linked to data taken from Moldova's online services

↳ *Source: The Record*

26k keys

live passwords and access keys (about 26,400) found in public code on Gitee

↳ *Source: MongoDB research blog*

JARGON BUSTER

Hot wallet: crypto kept online for fast payouts. Convenient, but reachable.

Management plane: the consoles that run a network. Own them, own the network.

Supply-chain attack: poisoning software you trust, so it arrives via a normal install.

THE REST OF THE WEEK

CONFIRMED INCIDENT · HEALTHCARE · LOGINS & ACCESS

A hospital pulled the plug in 40 minutes

Ambulances diverted, surgeries cancelled, claims still unverified.

> **AFFECTED** UNM Health (University of New Mexico Hospitals, US) · patients and staff · claimed by BYOD

WHAT: The state's only Level 1 trauma centre unplugged soon after a breach on 26 Oct. BYOD claims its identity tenant. UNM says core systems are safe.

LEADERS: Decide who can order a shutdown, and rehearse a day on paper.

TECH: Tier identity admin roles (PIM, phishing-resistant MFA) and alert on new federation or app consent.

HERE: GCC hospitals face the same call, and DoH Abu Dhabi expects tested continuity plans.

↳ *Source: Help Net Security · Infosecurity Magazine*

ACTIVELY EXPLOITED · CRITICAL INFRASTRUCTURE · NETWORK

Patched isn't the same as clean

State-backed crews are going after the boxes that run the network.

> **AFFECTED** Cisco SD-WAN and ASA/FTD customers · space, defence and policy targets · US utilities and telecom

WHAT: Talos tied KeyDrift malware, which copies SD-WAN encryption keys, to CVE-2026-20127. Lumen exposed Volt Typhoon's relay network.

LEADERS: After a critical network device is patched, ask for evidence it's clean.

TECH: Upgrade, lock management ports, hunt Talos indicators, rebuild if in doubt.

HERE: Run Cisco SD-WAN or ASA in the region? Patch, then hunt. Geo-blocking won't save you.

↳ *Source: The Hacker News (Cisco Talos, Lumen research)*

THE REST OF THE WEEK

CONFIRMED INCIDENT PUBLIC SECTOR · PERSONAL DATA

750,000 people, no login needed

Attackers used government services that never asked who was calling.

> **AFFECTED** Government of Moldova · 82 e-services checked (e.g. construction permits, medicine imports, food safety) · about 750,000 citizens

WHAT: Over five days, attackers sent about 11 million requests through Moldova's unauthenticated online services and linked systems. 82 services were checked and the vulnerable ones taken offline.

LEADERS: List every public service that returns personal data without a login, and ask who watches request volumes.

TECH: Require auth on data-returning APIs, rate-limit and alert on bulk queries, and test cross-system data paths.

HERE: GCC governments run many joined-up e-services. Any lookup API that skips login deserves the same review.

↳ *Source: The Record (Recorded Future News)*

NEXT FRONTIER

"Convenience" APIs that skip logins are the new open front door. Expect regulators to ask for an inventory of them.

FROM THE COMMENTS

Your comment could be here next Friday.

This week's question: if one laptop in your company were compromised tomorrow, what's the most it could move? Money, data or systems?

QUICK HITS

Six things in one minute

1 CERTIFICATES

eMudhra (emSign): eight certificate-authority keys could be worked out from public data. Browsers blocked them, but apps with built-in trust lists need rebuilding.

↳ *Source: The Hacker News*

2 LINUX SERVERS

Ubuntu and Red Hat servers: an old Linux TCP flaw (CVE-2026-98432) got an AI-built remote-root exploit in testing. Fixes still pending.

↳ *Source: The Hacker News · Cyber Kendra*

3 WEB & APPS

Node.js, Envoy, Istio, Bun and .NET: a Brotli flaw (CVE-2026-111497) with public exploit code. Patch, or block compressed request bodies.

↳ *Source: CIS MS-ISAC*

4 AI TOOLS

LiteLLM users: version 1.107.0 shipped with credential-stealing malware after its release pipeline was hijacked.

↳ *Source: BleepingComputer*

5 CLOUD TOOLS

OVHcloud CLI users: five GitHub releases were swapped for secret-stealing builds via a hijacked developer account.

↳ *Source: BleepingComputer*

6 SECRETS

Gitee (China's largest code host): 26,400 live keys found, incl. Alibaba Cloud, OpenAI and DeepSeek.

↳ *Source: MongoDB research blog*

NEW RULES, NEW TOOLS

What changed, what's worth a look

FRAMEWORK · NIST

NIST IR 8547: post-quantum roadmap

What changed: a roadmap to retire encryption that quantum computers could break, with full US federal migration by 2035.

Who: anyone using US-aligned vendors and products.

TRY IT 1. List the systems that encrypt data or use certificates.
2. Ask your top five vendors for their post-quantum plan.
3. Flag data that must stay secret for 10+ years (health, finance, IP).

↳ *Source: NIST*

TOOL · PUBLIC PREVIEW

GitHub npm package firewall

Does: blocks risky JavaScript packages at install time, incl. brand-new versions and new install scripts.

Vs. the rest: Socket, Snyk and JFrog cover more languages. GitHub's is built in but npm-only. Pricing not announced.

TRY IT 1. Pick one team's build pipeline on GitHub Enterprise Cloud.
2. Point its npm installs at the firewall instead of the public registry.
3. Set a 3–7 day cooldown, run a week, review what got blocked.

↳ *Source: The Hacker News*

YOUR WEEKEND PLAYLIST

Press play

Four picks · about 3 h in total · all cyber podcasts

66 MIN

RISKY BUSINESS · COMMUTE + LUNCH

#857: AI FUD intensifies

Patrick Gray with Alex Stamos · Risky Business Media

The week's supply-chain mess, incl. LiteLLM. Best for tech teams.

▶ risky.biz/RB857

80 MIN

DARKNET DIARIES · EVENING

#181: Ricky

Jack Rhysider · Darknet Diaries

How a phone hacker picked targets and broke in. Gripping for everyone.

▶ darknetdiaries.com/episode/181

27 MIN

BETWEEN TWO NERDS · AFTERNOON

Why frontier lab security will always suck

Tom Uren and The Grugq · Risky Business Media

Security culture at AI labs. Great for leaders vetting AI vendors.

▶ risky.biz/BTN187

8 MIN

RISKY BULLETIN · MORNING COFFEE

Brotli RCE is wrecking what's left of the internet

Risky Business Media news bulletin

A quick catch-up on the Brotli flaw. Tech.

▶ risky.biz/RBNEWS625

Full links are also in the first comment.

RABBIT HOLES

What to research next

Payment-request controls

Companies guard the keys that sign payments, but rarely limit which people and systems may *ask* for one. This is about mapping and capping those requesters.

WHY NOW Binance's keys were safe. A hijacked laptop made the request.

ASK Which of our systems will pay or export whatever a trusted service asks?

TRY Map one payment flow and mark every step a single approval can trigger.

Proving a network device is clean

After a patch, confirming no attacker code is left on a firewall, VPN or SD-WAN box, using logs, file hashes and integrity checks.

WHY NOW Cisco warns upgrades may not remove implants.

ASK What evidence would convince us a firewall is clean?

TRY For one firewall, list the logs and integrity checks you can collect today.

Package cooldowns

Making builds wait a few days before installing brand-new versions of open-source packages, so poisoned releases are caught first.

WHY NOW Poisoned LiteLLM and OVHcloud releases were caught within days.

ASK Could our builds wait 3–7 days for new versions?

TRY Run one team log-only for a week and count what a 3-day wait delays.

MONDAY CHECKLIST

Five things for Monday morning

Three for leaders, two for tech teams.

- [ ] LEADERS
Ask which systems can move money or data with a single approval

- [ ] LEADERS
Confirm who can order a shutdown, and when you last rehearsed it

- [ ] LEADERS
Ask key software suppliers how they protect their release process

- [ ] TECH
Patch Brotli in Node.js, Envoy and Istio, or block compressed request bodies

- [ ] TECH
After patching Cisco SD-WAN or ASA, hunt for implants and lock down management ports

Screenshot this page. Tick them off.

PICK A SIDE

Where do you land? Tell me in the comments.

THE SITUATION

You spot a live breach mid-morning on a busy weekday, as UNM Health did. What's your first move?

A

Pull the plug fast

Disconnect at the first sign of a breach, even if operations stop.

vs

B

Keep running, contain quietly

Isolate what's hit and keep services going while you investigate.

Or tell us how your team handled something similar. Leaders and tech folks both welcome.

See you next Friday.

Follow along and add your take below. The best comments make next week's issue.

↳ *Full source list and links in the comments · Curated by Ijaz · Views my own*