1.1 Million Cameras, One Wildcard

Architectural Surveillance in an IoT Cloud

DEF CON 34 · Main Stage

Sammy Azdoufal · @xn0tsa

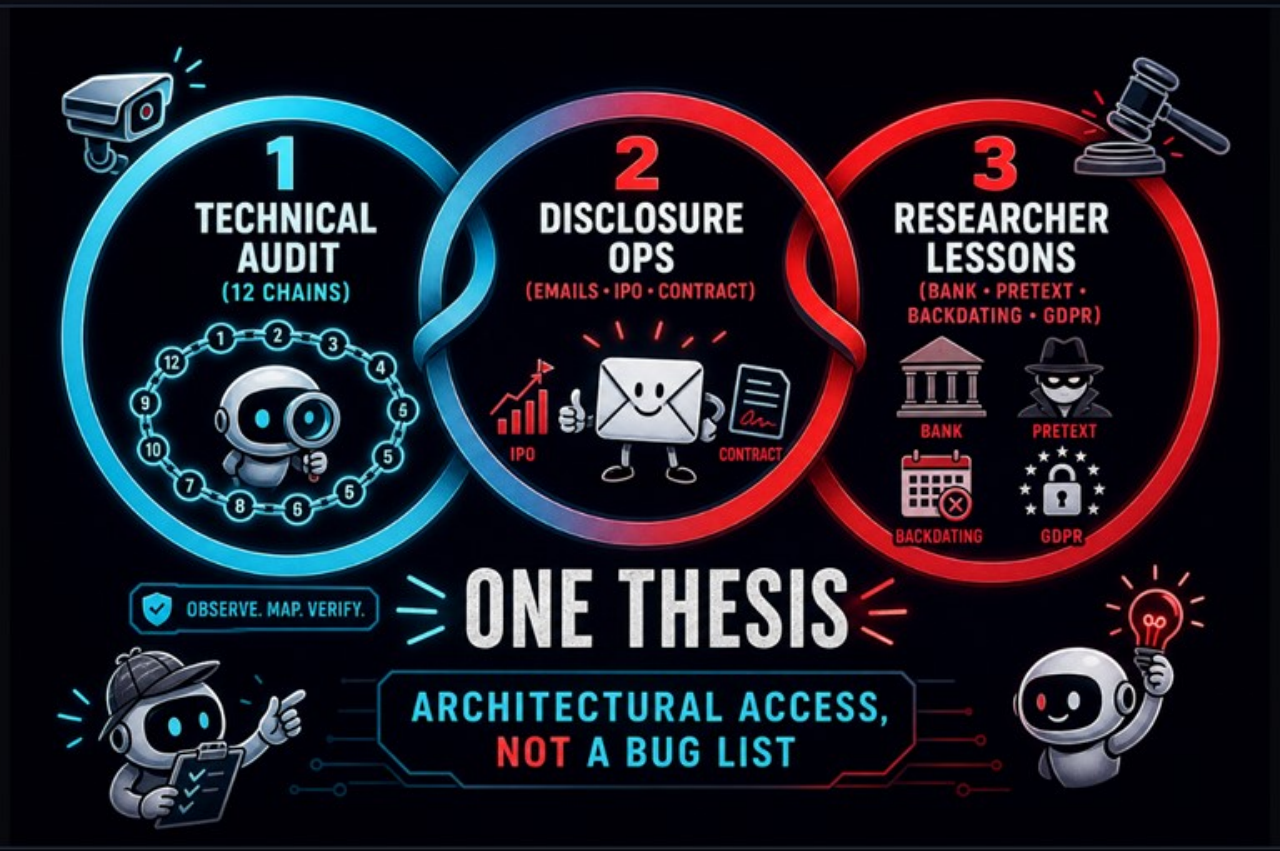
Not a bug talk. A receipts talk.

ONE WILDCARD

1.1 MILLION CAMERAS

“Most IoT talks end at the CVE.”

This one starts after the patch.



One thesis · three narratives: Audit · Disclosure ops · Researcher lessons.

The vendor has by-design access to every customer's camera.

Twelve independent chains.
Patch one — access remains.
Disclosure behavior is
chain thirteen.

Three stories. One thesis.

	Narrative	What it proves
1	**Technical audit**	Access is structural (12 chains — talk framing)
2	**Disclosure ops**	IR lag, backdating, the contract = evidence
3	**Researcher lessons**	Refuse the wrong instrument

If you can recite this table at the end, the talk worked.

SECTION 1 · 4 MIN · ORIGIN STORY

How I got here

Light foil → civilian question → Hangzhou.

Previously, on MQTT…

Two months earlier: **DJI ROMO** — same MQTT ACL smell, ~7k devices.

$30k. **One-page invoice.** No novel. We move on.

Then a colleague asked

Amazon baby monitor.

> “Is it safe?”

The box never names the cloud.
So I bought the same one.

Same smell. Different ending.

DJI paid like adults. **Meari** sent a Chinese-law service contract for the same neighborhood of money.

This talk is about the second ending.

SECTION 2 · 3 MIN

Meet the sticker farm

Meari in one breath

Hangzhou ODM. Camera + firmware + cloud + app. Partners slap a logo.

CloudEdge · Arenti · BOIFUN · PetTec · SV3C · Joystek · Luvion · …

IPO background: listed **March 9, 2025** (ChiNext). Share price doubled after listing.
Not a 2026 disclosure plot point — context.

Factory / assembly-line photo goes here — where the stickers get born.

Brand test

Watch DNS. `*.meari.com.cn` → you're in.
The logo on the plastic is cosplay.

You bought a brand. You rented an ODM camera cloud.

300+ logos. One SDK. One backend.

1.1M

devices · 118+ countries ·
registered at audit scale

SECTION 3 · 15 MIN · EVIDENCE CHAINS

Twelve chains. One access.

60–90 seconds each. Artifact → “why this alone is enough.”

How to listen to this section

Don’t collect CVEs like Pokémon.
Ask once per chain: if this were the only finding — does the vendor still have a path to the camera?
Twelve yeses = architecture.

Evidence board

01–06 firehose · secret store · forever JPEGs · XOR costume · CMS · DingTalk SSO
07–12 OpenAPI WAN-IP · TUTK · PIS bulk · RSA unbind · cloud-video (withdrawn) · static keys

Talk framing = **12 evidence chains**. CVE numbers at the end of this section — not the point of each slide.


DEFAULT CREDENTIALS
NORTH AMERICA ONLINE
EUROPE ONLINE
SOUTH AMERICA ONLINE
ASIA / PACIFIC ONLINE
Customer Portal
https://totally.secure.login
PLEASE SIGN IN
Username
admin
Password
public
ACCESS GRANTED
Welcome, admin!
You now have full access to everything.
ZERO ALERTS CLUB
SECURITY? NAH.
TODO:
• FIX LATER
• SECURITY
IT WORKS ON MY MACHINE
HACKER OF THE MONTH*
* BY DEFAULT
DEPLOY & PRAY
IN PRODUCTION, ON FOUR CONTINENTS.

01 EMQX — the welcome mat

Regional brokers (US-West · EU-Frankfurt · CN-Hangzhou · + Global/HK path).
Dashboards on `:18083`. Default `admin:public`. Auth plugins off.
Wildcard subscribe: yes. Anonymous: yes.

Alone: still a vendor path? **Yes.**

Wildcard topic on an authenticated free account = the firehose.
(Historical finding — don't "try it from the hotel.")

`14,204 msgs / 5 min · 2,117 devices · one free account`

02 Apollo — secret vending machine

Port 8080. No auth.
614 prod keys across 11 microservices: DB roots, Redis, MQTT globals, DingTalk, RSA unbind, OAuth…

Config server ≠ junk drawer. Apparently nobody told them.

03–04 Pictures or it didn't happen

03 Shared OSS · no isolation · no expiry · URL on MQTT
04 Baby/indoor `.jpgx3` = XOR first 1KB · SN in the same message

Calling XOR "encryption" is a lifestyle brand.

Real alert still goes here — faces / IDs redacted. Swap file when ready.

“Encryption as a lifestyle brand.”

SN in the clear. XOR on the first kilobyte. Fashion.

Montage slot: baby · doorbell · indoor · factory line.

05–06 Humans in the loop (the scary kind)

05 CMS operator routes: live / playback / snapshot / cloud video…
06 DingTalk creds in Apollo · **678** employees · SSO path into the console

Corporate chat as a door into the operator camera desk.

SSO into the camera desk.

678 employees. QR scan.
Wrong blast radius.

07–08 Serial → network path

07 Hardcoded OpenAPI HMAC in every APK → **device status / WAN IP by serial**
08 Universal TUTK authcode → direct P2P (cloud optional) — structural only

Alone: still a vendor path? **Yes.** Not a hotel CTF handout.

09–12 Industrialize it

09 PIS bulk P2P list — **1.16M US P2P rows (+98k Hangzhou)**
10 RSA unbind private key (from Apollo)

11 Cloud-video `/detail` — **withdrawn after re-test** (methodology lesson only)
12 Static keys across every brand — rotate = break 1.1M devices

Alone: still a vendor path? **Yes** (11 kept as “how re-tests lie”).

Twelve yeses.

That’s architecture. Not a CVE zoo.

The five that got numbers

CVE-2026-**33356** · **33357** · **33359** · **33361** · **33362**

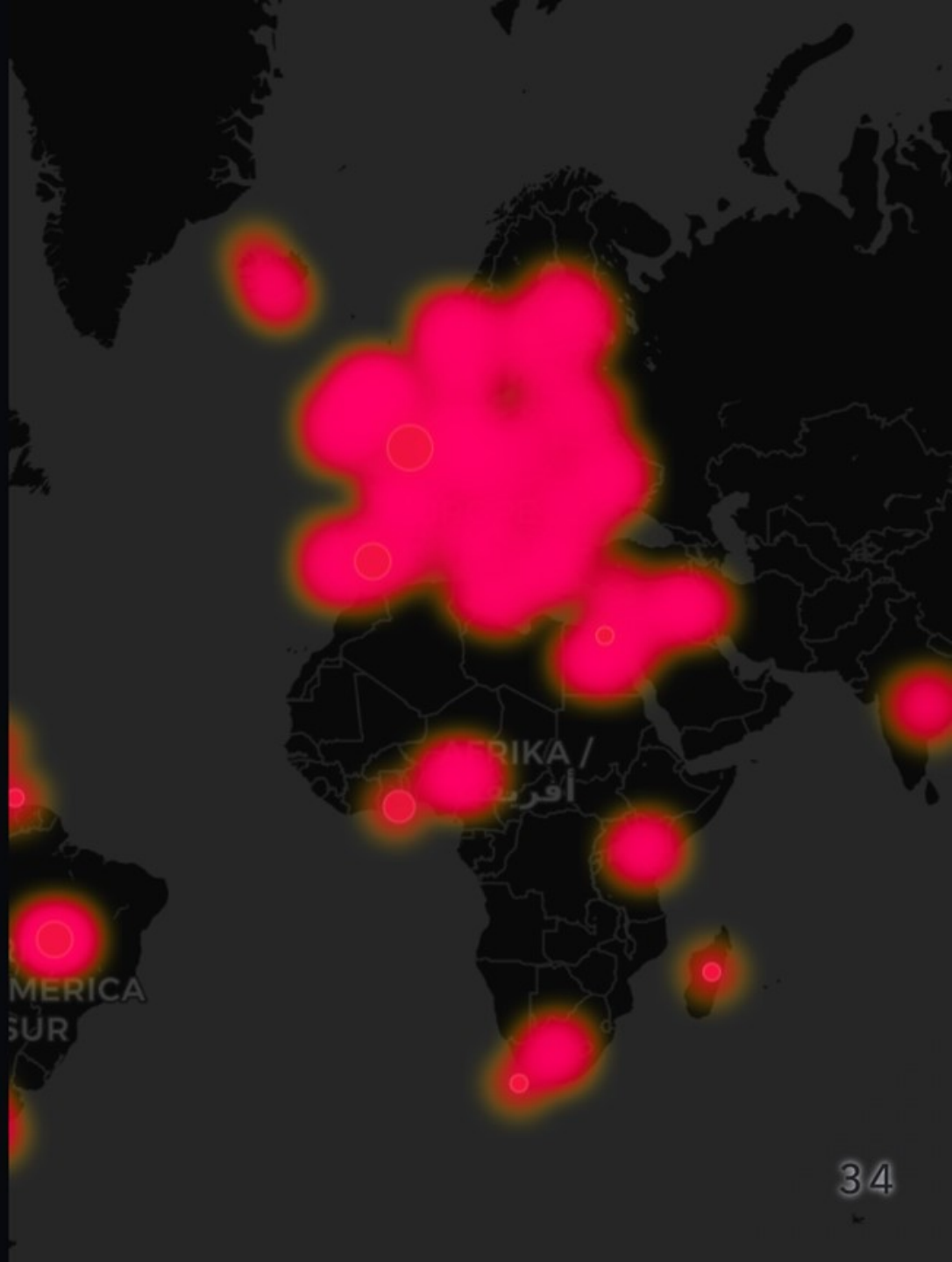
runZero (Tod Beardsley) · CISA coordinated.

Five CVE IDs in the public writeup. Twelve chains = talk/audit framing (not a numbered board in the disclosure). Cloud-video withdrawn from CVE set; CN sig bypass too — Q&A if you care.

The map is not vibes

~826k devices by WAN IP.

When the architecture is the exploit, the heatmap is the CVSS.



Live bit / tape bit

1. **Tape:** 30s sanitized MQTT wildcard (PII redacted) — historical audit window
2. **Live:** EMQX dashboards **firewalled** 👏 (port block — `admin:public` never rotated)
3. **Residual (audit IR):** Apollo MQTT creds still worked on **3/4** brokers after dashboards went dark
4. **Apollo HTTP** 401 only as of **talk prep** — separate from the 5-day story

They patched the welcome mat. Kept the firehose keys.

IR lag is a finding.

HK dashboards ~24h. US/EU ~5 days later. Apollo stayed open the whole assessment.

SECTION 4 · 10 MIN · THE FUN PART (FOR LAWYERS)

Disclosure ops

Emails as exhibits. Popcorn optional.

Greatest hits playlist

Beat	Line
Mar 2	HK locks `:18083` in 24h — US/EU wait **5 days**
Mar 12	“obsolete products” + $15k if I **delete the internet**
Mar 12–13	I delete posts anyway (users > clout) · tone shift “unlawful”
Mar 15	$30k offer + “technical partnership” article pitch + GDPR vibes
Apr 4 (Day 24)	Advisories published, **stamped Mar 2** (Wayback: lol no)
Apr 16→25	PRC service contract → I refuse → one-page VDRA
May 11	Full public disclosure

VENDOR EMAIL

ALSO STILL ON SALE

> **The products affected are our obsolete products.**

Amazon checkout still worked. Amazing obsolescence.

Backdating speedrun

Published **April 4**. Stamped **March 2**.
Nine days before first contact.

Wayback + DNS history: pages didn’t exist on Mar 2.
Covered **3 of 11** findings reported (not the full CVE set).
Apollo = “a limited amount of configuration information.”

`archive.org = offensive security tool.`

SAME BOUNTY. DIFFERENT VIBES.

Same $30k neighborhood. Opposite movie.

DJI: one-page invoice. Paid.
Meari: Personal Service Contract —

- PRC law / Chinese courts
- Refund clause at their discretion
- No right to publish
- You eat the tax (incl. China)

That's not banking. That's a leash.

Art. 33 / 34 asked. Vibes answered.

May 11 energy

Refuse the novel → propose one-page VDRA.
Public ships **5 CVEs + other findings + timeline** — not a numbered 12-chain board.
Twelve chains = talk / private audit framing. Publish. runZero · CISA.

The disclosure date was never the negotiation chip.

SECTION 5 · 8 MIN · STEAL THIS

Three lessons

Narrative 3. Screenshot fuel.

1. “The bank needs a service contract”

Test it.

SAFE under $50k → invoice + purpose declaration.
Not a refundable no-publish PRC novella.

Side-by-side on screen: DJI form vs Meari contract.
Audience does the math.

2. Backdated advisories are a lab method

1. Wayback the URL
2. DNS history
3. Vendor social announce
4. Email headers / first-fix date

If the stamp predates first contact: **say it with charts.**

3. GDPR Art. 33 is a crowbar

EU data exposed + vendor won’t notify?
AEPD / CNIL don’t need your bounty contract.

File the week you publish.
The complaint is part of the research corpus.

CLOSE · 5 MIN + Q&A

What to remember walking out

Big picture, one more time

Architectural / by-design access — twelve independent chains (talk / private audit framing).

1	**Audit** — the chains (not the public CVE count)
2	**Disclosure ops** — evidence too
3	**Researcher lessons** — refuse the leash

ONE WILDCARD

1.1 MILLION CAMERAS

Patch the bug.
Keep the architecture.
Call it remediated.

Don’t clap for that.

One wildcard. 1.1M cameras.

Sammy Azdoufal · @xn0tsa

Disclosure repo linked in the talk notes / QR

Questions that don’t create victims tonight