Coordinated Security & Privacy Disclosure, Final Report

XTrend Speed for Android (com.rynatsa.xtrendspeed)

Eleven written notices, ninety-one days, one working channel found by elimination, zero replies of any kind

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINE FINDINGS UNADDRESSED, INCLUDING TWO CRITICAL RCE-CLASS EXPOSURES ON A REGULATED TRADING APP

Target	Rynat Capital (Rynat SA), Cyprus Investment Firm license 303/16, CySEC-regulated
Product audited	XTrend Speed for Android, com.rynatsa.xtrendspeed, v2.0.7
Disclosure reference	REF: com.rynatsa.xtrendspeed
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 hardcoded Firebase key with live database URL, CVSS v4.0 9.3; H1 bundled FastJSON RCE-class CVEs, CVSS v4.0 9.2, both unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production XTrend Speed Android application, a CFD/forex trading app operated by Rynat Capital, a CySEC-regulated Cyprus Investment Firm, and identified nine findings: global cleartext traffic permitted for financial transactions, a hardcoded Firebase API key with a live database URL, a bundled Alibaba FastJSON library carrying multiple deserialization RCE CVEs including CVE-2022-25845 (CVSS 9.8), a Facebook SDK relaying trading behavior to Meta's advertising infrastructure with no disclosed MiFID II Art. 27 conflict-of-interest assessment, an AppsFlyer OAID Chinese device-fingerprinting SDK collecting persistent identifiers with no GDPR Art. 6(1) basis for EU users, a minSdk of 21 (Android 5.0, 2014) compounding the cleartext exposure on unpatched devices, a debug Google OAuth client ID shipped in the production binary, an overlay-attack surface on trade-confirmation and withdrawal screens with no legitimate CFD use case, and an undisclosed white-label trading codebase attributed to an unnamed Chinese vendor operating as 'Trade Eight', undisclosed to users or to CySEC under MiFID II Art. 24(5).

Delivery itself proved adversarial. R1's initial cc addresses included a misspelled complaints mailbox at Rynat Capital and legal@xtrendspeed.com, both of which bounced immediately, as did an attempted regulator bcc to CySEC's postmaster address. RFI-IRFOS re-sent to confirmed-live addresses only and, from 4 July 2026 onward, cc'd the Austrian Datenschutzbehörde and CERT.at throughout. Across eleven written notices over ninety-one days, including a day-59 message with a hard 25 August 2026 deadline on three yes/no questions and a final pre-embargo notice on 16 September 2026, no reply of any kind, automated bounce aside, was ever received from any address at XTrend Speed or Rynat Capital.

None of the nine findings were confirmed, disputed, or otherwise addressed. In particular, whether CySEC was notified of the cleartext-traffic exposure, whether the Austrian lead supervisory authority was notified under Art. 33 GDPR within 72 hours of RFI-IRFOS's disclosure, and whether the FastJSON RCE-class dependency has been patched or removed remain fully open questions on a regulated retail trading platform as of the embargo date.

Scope: Static analysis of the publicly downloaded production XTrend Speed Android APK (v2.0.7), on an authorized test device, only. No XTrend Speed account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to support@xtrendspeed.com, funding@xtrendspeed.com, and a misspelled complaints address at Rynat Capital that bounced immediately, along with legal@xtrendspeed.com and postmaster@cysec.gov.cy, both of which also bounced. Across eleven written notices over ninety-one days, spanning two Gmail threads after a subject-line change, no reply of any kind, automated or human, was ever received from support@xtrendspeed.com, funding@xtrendspeed.com, info@rynatcapital.com, or complaints@rynatcapital.com.

ID	Severity	Title
C1	HIGH	Global cleartext traffic permitted, financial data transmitted over HTTP
C2	CRITICAL	Hardcoded Firebase API key with a live database URL
H1	CRITICAL	Alibaba FastJSON bundled, multiple RCE-class CVEs
H2	MEDIUM	Facebook SDK and AppEvents on a MiFID II-regulated trading platform
H3	HIGH	AppsFlyer OAID, Chinese device-fingerprinting SDK, no GDPR basis
H4	LOW	minSdk 21 (Android 5.0, 2014) compounding the cleartext exposure
H5	MEDIUM	Debug Google OAuth client ID shipped in the production binary
H6	MEDIUM	SYSTEM_ALERT_WINDOW, overlay-attack surface on trade-confirmation screens
H7	MEDIUM	Undisclosed white-label trading codebase from an unnamed Chinese vendor

Subject & Operator Analysis

Rynat Capital (Rynat SA) is a Cyprus Investment Firm holding CySEC license 303/16, operating the XTrend Speed retail CFD/forex trading platform, under the direct jurisdiction of the Cyprus Securities and Exchange Commission and, for EU users, the GDPR lead supervisory authority regime.

Findings

C1: Global cleartext traffic permitted, financial data transmitted over HTTP

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6

network_security_config.xml declares a base-config with cleartextTrafficPermitted="true". Login credentials, deposits, withdrawals, and trading positions may be transmitted unencrypted.

No reply of any kind addressed this finding across eleven notices. Whether CySEC has been notified of this exposure on a regulated trading platform remains an open question.

Impact: On any network segment along the transmission path, credentials, deposits, withdrawals, and live trading positions on a regulated CFD platform can be intercepted or manipulated in plaintext.

Fix: Remove cleartextTrafficPermitted from the base network security configuration and enforce TLS for all traffic, with certificate pinning for authentication and transaction endpoints.

C2: Hardcoded Firebase API key with a live database URL

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N, 9.3

res/values/strings.xml contains google_api_key (AIzaSyC4GOmuRqkW2nZy0L_Yl55qRkjUTEejhtw), firebase_database_url (https://xtrend-speed.firebaseio.com), google_app_id, and project_id (xtrend-speed), all extractable from the public APK in under 30 seconds.

Unlike a bare project key, a hardcoded firebase_database_url points directly at a specific Realtime Database instance; whether its security rules are deny-by-default cannot be verified externally, and no reply addressed this. No reply of any kind addressed this finding across eleven notices.

Impact: If the referenced Realtime Database's rules are not deny-by-default, this key and URL combination permits direct external read or write access to a financial application's backend data store.

Fix: Rotate the exposed key, confirm Realtime Database security rules are deny-by-default, and remove the hardcoded database URL from the client binary.

H1: Alibaba FastJSON bundled, multiple RCE-class CVEs

CRITICAL, CVSS v4.0 AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N, 9.2

Alibaba FastJSON (76 classes) is bundled, a library associated with multiple deserialization remote-code-execution CVEs, including CVE-2022-25845, CVE-2017-18349, and CVE-2022-25897, several independently rated CVSS 9.8 by their original disclosers.

RFI-IRFOS's static analysis cannot confirm whether a reachable deserialization entry point exists in XTrend Speed's specific integration; this finding is scored conservatively (AC:H) to reflect that unconfirmed reachability, not as a verified live exploit. Whether this dependency has been patched or removed was asked repeatedly and never answered.

Impact: A financial services application bundling a library with multiple independently-rated CVSS 9.8 deserialization RCE CVEs carries unresolved remote-code-execution risk pending confirmation that no reachable vulnerable code path exists.

Fix: Upgrade or remove the FastJSON dependency, and confirm no vulnerable deserialization entry point is reachable from untrusted input.

H2: Facebook SDK and AppEvents on a MiFID II-regulated trading platform

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9

Trading behavior, login, deposit, trade execution, and profit-and-loss views, is sent to Meta's advertising infrastructure via the Facebook SDK and AppEvents.

RFI-IRFOS asked whether this data flow was assessed against MiFID II Art. 27's conflict-of-interest obligations; no reply addressed this question.

Impact: Retail trading behavior on a regulated platform is shared with a third-party advertising network with no disclosed conflict-of-interest assessment.

Fix: Remove or restrict Facebook AppEvents from trading-behavior events, and document a MiFID II Art. 27 assessment for any retained advertising data flow.

H3: AppsFlyer OAID, Chinese device-fingerprinting SDK, no GDPR basis

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7

OAID (MSA), a Chinese-originated device-identification standard, is present via 20 classes collecting persistent device identifiers.

RFI-IRFOS asked what Art. 6(1) legal basis applies to this collection for EU users; no reply addressed this question across eleven notices.

Impact: A persistent, China-linked device identifier is collected from EU users with no confirmed lawful basis or disclosed transfer mechanism.

Fix: Confirm the Art. 6(1) legal basis for OAID collection on EU users, or remove the SDK for that user population.

H4: minSdk 21 (Android 5.0, 2014) compounding the cleartext exposure

LOW, CVSS v4.0 AV:A/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.3

The app supports Android 5.0 (API 21), a twelve-year-old, long-unpatched platform baseline, combined with the C1 cleartext-traffic permission.

A retail investor on an Android 5 device connected to unsecured Wi-Fi transmits trading positions in plaintext, on a device that cannot receive current platform security patches. Never addressed in any reply.

Impact: Compounds C1's exposure on the platform's oldest supported devices, where OS-level mitigations are unavailable.

Fix: Raise minSdk to a currently-patched Android baseline in line with the app's risk profile.

H5: Debug Google OAuth client ID shipped in the production binary

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.3

google_server_client_id_debug is present in the production build, indicating inadequate separation between debug and release build pipelines.

Never addressed in any reply.

Impact: Debug-scoped OAuth configuration shipping in production release configuration is a build-hygiene gap that can carry unintended authentication surface.

Fix: Strip debug-scoped identifiers from the release build pipeline before publishing to production.

H6: SYSTEM_ALERT_WINDOW, overlay-attack surface on trade-confirmation screens

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N, 6.8

SYSTEM_ALERT_WINDOW is requested with no legitimate CFD trading use case identified, creating overlay-attack surface on withdrawal and trade-confirmation flows.

Never addressed in any reply.

Impact: A co-located malicious app could overlay withdrawal or trade-confirmation screens to manipulate what a user believes they are confirming.

Fix: Remove SYSTEM_ALERT_WINDOW unless a specific, documented trading feature requires it, and harden confirmation screens against overlay attacks (FLAG_SECURE, touch filtering).

H7: Undisclosed white-label trading codebase from an unnamed Chinese vendor

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.9

com.trade.eight (~700 classes) and com.easylife.ten indicate the actual trading engine is white-label software built by an undisclosed Chinese vendor operating as 'Trade Eight', not disclosed to users or, so far as RFI-IRFOS could determine, to CySEC.

Never addressed in any reply. Raises both a GDPR Art. 13(1)(a) processor-disclosure question and a MiFID II Art. 24(5) information-to-clients question.

Impact: Retail clients on a CySEC-regulated platform are trading through an undisclosed third-party engine whose data-handling practices have not been named or assessed.

Fix: Disclose the white-label vendor relationship to users and to CySEC, and confirm what data the vendor's engine processes or retains.

Eleven Notices, a Broken Complaints Address, and Total Silence

This case's delivery record is itself notable: R1's complaints address at Rynat Capital was misspelled and bounced immediately, legal@xtrendspeed.com bounced on every attempt, and an attempted regulator bcc to CySEC's own postmaster address bounced as well. RFI-IRFOS re-sent to the two confirmed-live addresses, support@xtrendspeed.com and fund ing@xtrendspeed.com, and from 4 July 2026 cc'd the Austrian Datenschutzbehörde and CERT.at throughout. Across eleven notices over ninety-one days, including a hard 25 August 2026 deadline on three yes/no questions and a final pre-embargo notice on 16 September 2026, no reply of any kind, human or automated, was ever received.

Data Protection & MiFID II, Provision by Provision

Finding	Provision	Concern
C1	GDPR Art. 32	Cleartext-permitted financial transactions, unaddressed
C2	GDPR Art. 32	Hardcoded Firebase key with live database URL, unaddressed
H1	GDPR Art. 32	Bundled RCE-class dese-rialization library, unad-dressed
H2	MiFID II Art. 27	Trading behavior shared with advertising infras-tructure, no conflict-of-i nterest assessment
H3	GDPR Art. 6(1)	Chinese device-fingerpr inting SDK, no lawful ba-sis for EU users
H7	GDPR Art. 13(1)(a), MiFID II Art. 24(5)	Undisclosed white-label trading engine vendor

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent; complaints@rynatcapital.com (misspelled), legal@xtrendspeed.com, and postmaster@cysec.gov.cy all bounce
2026-06-27	Re-sent to confirmed-live addresses only, bcc dsb@dsb.gv.at and cert@cert.at
2026-07-04	Embargo first stated explicitly as 2026-09-19; three standing questions posed; a paid NDA engagement offer was also included in this and later notices, historical record only, not a currently open offer
2026-07-17	Day 27 silence follow-up
2026-08-09	Day 17 follow-up 'at the only working channel'
2026-08-18	Day 59 follow-up, three yes/no questions, deadline of 2026-08-25
2026-09-04	Day 77 follow-up, 25 August deadline passed with no reply
2026-09-12	Day 84 follow-up, 'Embargo in 7 Days'
2026-09-16	Final pre-embargo notice, 'Question Deadline Reached Today'
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Remove cleartextTrafficPermitted and enforce TLS with certificate pinning for all authentication and transaction traffic.
- Rotate the exposed Firebase key and database URL, and confirm Realtime Database security rules are deny-by-default.
- Upgrade or remove the bundled FastJSON dependency and confirm no reachable deserialization entry point exists.
- Disclose the white-label trading-engine vendor relationship to users and to CySEC.
- Confirm whether CySEC and the GDPR lead supervisory authority have been notified of these findings.

RFI-IRFOS rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Coordinated disclosure per ISO/IEC 29147. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 6, 13, 32, 33, 44. MiFID II Art. 24, 27. REF com.rynatsa.xtrendspeed.