Coordinated Security & Privacy Disclosure, Final Report

SHEIN for Android (com.zzkko)

Certificate pins expired for 33 months and silently disabled, eight notices, only automated routing guides in reply

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY DAYS, ZERO SUBSTANTIVE REPLIES OF ANY KIND

Target	Roadget Business Pte. Ltd. (Singapore) / SHEIN Distribution EU B.V. (Netherlands)
Product audited	SHEIN for Android, com.zzkko
Disclosure reference	REF SHEIN-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 Firebase key / C2 expired certificate pins, CVSS v4.0 9.3)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

1 Executive Summary 3

2 Subject & Operator Analysis 4

3 Positive Observations 4

4 Findings 4

4.1 C1: Hardcoded Firebase API key in the production APK 4

4.2 C2: Certificate pin set expired 33 months ago, silently disabling pinning, with global cleartext permitted 5

4.3 H1: Facebook Conversions API: fashion purchase data enabling body and lifestyle inference 6

4.4 H2: AppsFlyer: purchase events and device identifiers to a US attribution platform 6

4.5 H3: READ_CALENDAR and WRITE_CALENDAR permissions, undisclosed purpose on a shopping app 7

4.6 H4: requestLegacyExternalStorage bypasses Android's scoped storage model 7

4.7 H5: Corporate structure and China's National Security Law: compelled-disclosure exposure 7

5 Data Protection, Article by Article 8

6 Disclosure Timeline & Outcome 9

7 Residual Risk & Recommendations 10

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production SHEIN Android application and identified seven findings, two CRITICAL, five HIGH. The most significant: the app's certificate pin set expired in October 2024, roughly 33 months before this report's publication, with no overridePins attribute set, which silently disables certificate pinning entirely rather than failing closed, and cleartextTrafficPermitted is set to true in the base network security configuration, permitting unencrypted HTTP to any non-shein.com endpoint.

A hardcoded Firebase API key was also extracted from the production binary. Five further findings raise separate concerns: Facebook Conversions API transmitting fashion purchase data enabling body-metric inference; AppsFlyer transmitting purchase events and device identifiers to a US attribution platform; undisclosed calendar read/write access on a shopping app; unscoped external storage access bypassing Android's scoped storage model; and a corporate structure question regarding China's National Security Law given the company's beneficial ownership.

Eight written notices were sent over 90 days, across addresses that shifted as earlier ones were reported discontinued mid-campaign. Every reply received was either an automated mailbox-discontinued notice or an identical automated customer-service routing guide. No human at SHEIN ever engaged with a single finding. All seven findings stand exactly as originally reported.

Scope: Static analysis of the publicly downloaded production SHEIN Android APK, on an authorized test device, only. No SHEIN account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to privacy@shein.com and privacy@sheingroup.com, cc security@shein.com, bcc the Austrian DSB, CERT.at, and the EDPB. Four further written notices followed through 4 September 2026, routed to updated addresses as earlier ones were reported discontinued. Every reply received, from legal@shein.com and media@sheingroup.com, was an identical automated customer-service routing guide or a mailbox-discontinued notice. No human ever engaged with the findings.

ID	Severity	Title
C1	CRITICAL	Hardcoded Firebase API key in the production APK
C2	CRITICAL	Certificate pin set expired 33 months ago, silently disabling pinning, with global cleartext permitted
H1	HIGH	Facebook Conversions API: fashion purchase data enabling body and lifestyle inference
H2	HIGH	AppsFlyer: purchase events and device identifiers to a US attribution platform
H3	HIGH	READ_CALENDAR and WRITE_CALENDAR permissions, undisclosed purpose on a shopping app

ID	Severity	Title
H4	HIGH	requestLegacyExternalStorage bypasses Android's scoped storage model
H5	HIGH	Corporate structure and China's National Security Law: compelled-disclosure exposure

Subject & Operator Analysis

Roadget Business Pte. Ltd. (Singapore), part of SHEIN Group Ltd., operates the SHEIN Android application for EU users through SHEIN Distribution EU B.V. (Netherlands).

Positive Observations

No specific positive controls were identified as a distinct section in the original disclosure; the audited binary's primary characteristics are addressed directly in the findings above.

Findings

C1: Hardcoded Firebase API key in the production APK

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

API key AIzaSyBaVm1lHHfTiZzeVqwId5Fs2ThFiTDbU4o, project shein-3876, extracted from res/values/google-services.xml.

No response was received naming this finding.

Impact: A publicly extractable production credential enables probing of the project and potential further backend access.

Fix: Rotate the key and restrict it to the com.zzkko package and certificate fingerprint.

C2: Certificate pin set expired 33 months ago, silently disabling pinning, with global cleartext permitted

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

The network security configuration pins shein.com with four SHA-256 pins expiring 2024-10-07, with no overridePins attribute set. base-config sets cleartextTrafficPermitted="true".

```
<base-config cleartextTrafficPermitted="true" />
<domain includeSubdomains="true">shein.com</domain>
<pin-set expiration="2024-10-07">
  PvSdSRLbnVwPKahvI1+kmhcVo7E2McODaQd/5laciUA=
  3mc/12C2pwvtV5JjfcxLmbbWYQSbj9yqSWLXKfZcMUw=
  20I2I65F+H8zQpYs/0c1KyGAF5PGgnBVROHxceMf8jk=
  RQeZkB42znUfsDIIFWIRiYEcKl7nHwNFwWCrnMMJbVc=
</pin-set>
```

No response was received naming this finding, including the direct question of whether the pin set has ever been renewed. On Android, an expired pin set with no overridePins attribute causes pinning to fail open silently, no exception, no user warning, no app-side detection. As of the original disclosure this had already lapsed over 20 months; by the final follow-up RFI-IRFOS states 33 months. Cleartext being simultaneously permitted globally means any non-shein.com endpoint, analytics, CDNs, third-party SDKs, may be reached over unencrypted HTTP.

Impact: Certificate pinning has been non-functional for nearly three years with no detection mechanism, and cleartext HTTP is permitted globally, exposing all non-primary-domain traffic to interception on untrusted networks.

Fix: Renew the certificate pin set immediately, set overridePins appropriately, and set cleartextTrafficPermitted to false globally.

H1: Facebook Conversions API: fashion purchase data enabling body and lifestyle inference

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

AppEventsConversionsAPITransformer and ConversionsAPIEventName classes send fashion purchase data, items, sizes, categories, to Meta advertising infrastructure.

No response was received naming this finding. Purchase data from a predominantly female EU user base, including size and category information, enables body-metric and socioeconomic inference by a third-party advertising platform.

Impact: Fashion purchase data capable of supporting body-metric inference is transmitted to a third-party advertising platform with no disclosed specific consent basis for this inference risk.

Fix: Disclose the Conversions API data flow explicitly and its inference implications under Art. 13(1)(e), and confirm the Art. 46 transfer mechanism.

H2: AppsFlyer: purchase events and device identifiers to a US attribution 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

The com.appsflyer package transmits install referral data, purchase events, and the Google Advertising ID to a US attribution platform.

No response was received naming this finding.

Impact: Device identifiers and purchase behavior enable cross-app behavioral profile linkage with no confirmed Art. 46 transfer safeguard.

Fix: Disclose AppsFlyer as a named data recipient under Art. 13(1)(e) and publish its transfer mechanism.

H3: READ_CALENDAR and WRITE_CALENDAR permissions, undisclosed purpose on a shopping app

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

The app requests READ_CALENDAR and WRITE_CALENDAR, granting access to appointment titles, locations, medical appointments, and travel plans.

No response was received naming this finding, including the direct question of the disclosed purpose. This is data far beyond delivery-reminder functionality on a fashion shopping app.

Impact: Broad calendar read/write access, including potentially medical or travel-related appointment data, is granted with no disclosed shopping-app purpose.

Fix: Replace calendar permission usage with Intent.ACTION_INSERT, which requires no permission, or disclose the specific purpose under Art. 13.

H4: requestLegacyExternalStorage bypasses Android's scoped storage model

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

android:requestLegacyExternalStorage="true" bypasses Android 10's scoped storage model on Android 10 and 11 devices, granting unscoped read access to all files on external storage, including files belonging to other apps.

No response was received naming this finding.

Impact: On affected Android versions, the app can read files belonging to other installed applications with no scoping restriction.

Fix: Migrate to scoped storage APIs and remove the legacy flag.

H5: Corporate structure and China's National Security Law: compelled-disclosure exposure

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

SHEIN Group Ltd. is Singapore-registered with a beneficial owner named in RFI-IRFOS's correspondence as Xu Yangtian (also referenced as Xu Yangchun), raising a PRC corporate-structure question distinct from the app's technical findings.

No response was received naming this finding. RFI-IRFOS's position: this corporate structure carries potential exposure under China's National Security Law Art. 7, which can compel cooperation with state intelligence access requests, independent of where the app's servers are physically located.

Impact: A structural transfer-risk question exists regarding potential compelled data access, independent of and in addition to the app's specific technical findings.

Fix: Publish a clear statement on corporate structure, beneficial ownership, and the specific Art. 46 safeguards applicable to any data access originating from PRC-linked corporate entities.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32	Hardcoded, publicly extractable credential
C2	GDPR Art. 25, Art. 32(1)(a), Art. 5(1)(f)	Certificate pinning silently non-functional for 33 months, global cleartext permitted
H1	GDPR Art. 6(1)(a), Art. 13(1)(e), Art. 46	Purchase data enabling body-metric inference to a third party
H2	GDPR Art. 6(1)(a), Art. 28, Art. 46	Undisclosed US attribution processor
H3	GDPR Art. 5(1)(c), Art. 13	Undisclosed calendar access
H4	GDPR Art. 5(1)(c)	Unscoped external storage access
H5	GDPR Art. 44, Art. 46	Corporate structure, potential compelled-disclosure exposure

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to privacy@shein.com and privacy@sheingroup.com, cc security@shein.com, bcc Austrian DSB/CERT.at/EDPB, 7 findings
2026-06-28	Follow-up #1, 7 days no reply, three questions posed
2026-07-27	Follow-up #2, resent to updated addresses after privacy@shein.com reported discontinued; automated mailbox-phased-out and customer-service routing-guide replies received
2026-08-25	Follow-up #3, 65 days, states certificate pinning non-functional 22+ months at that point; weekly APK diffing instituted; identical automated replies received
2026-09-04	Follow-up #4, 68 days, restates all findings, poses three new questions including who the named contact is; identical automated replies received
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Eight written notices across 90 days, sent to shifting addresses as earlier ones were reported discontinued mid-campaign, produced only automated mailbox-phased-out notices and an identical customer-service routing guide. No human at SHEIN ever engaged with any of the seven findings, including the specific and repeated question of who the named contact for this disclosure is.

Residual Risk & Recommendations

- Renew the certificate pin set immediately and set cleartextTrafficPermitted to false globally; this is the single highest-priority item given nearly three years of silent non-functionality.
- Rotate the Firebase key and restrict it to the production certificate fingerprint.
- Disclose the Facebook Conversions API and AppsFlyer data flows as named recipients with their transfer mechanisms.
- Remove or disclose the specific purpose of calendar access, and migrate away from legacy unscoped external storage.
- Publish a clear statement on corporate structure and beneficial ownership, and confirm which supervisory authority has been notified under Art. 33 given the multi-year certificate-pinning failure.
- Establish a working, staffed reply path for security and privacy disclosures independent of the automated inboxes encountered throughout this case.

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, 25, 28, 32, 44, 46. REF SHEIN-2026-R1.