Coordinated Security & Privacy Disclosure, Final Report

Nike for Android (com.nike.omega)

Live dev and production push credentials, hundreds of millions of devices, eighty-three days, nine notices, zero replies

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

Target	Nike, Inc., Beaverton, Oregon, US
Product audited	Nike for Android, com.nike.omega, v26.31.2
Disclosure reference	REF NIKE-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 Firebase/Maps keys, C2 Airship push credentials, 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

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production Nike Android application and identified six findings, two CRITICAL, four HIGH. The most significant: both the development and production Airship push credentials are hardcoded in the production APK's own configuration file, alongside an inProduction=false flag the file's own comment instructs be set to true before app-store submission. Extracting either credential enables sending push notifications to Nike's entire subscriber base, stated at potentially hundreds of millions of devices, and reading notification analytics and user tags including sneaker preferences and loyalty status.

Separately, a hardcoded Firebase API key and Google Maps key were extracted from the production binary, along with four further findings: Forter, a cross-merchant fraud-scoring SDK not named as a data processor and implicated in undisclosed Art. 22 automated decision-making; undisclosed Airship geofencing and Bluetooth beacon detection; Singular cross-app advertising attribution; and New Relic HTTP capture including purchase-flow request details.

Nine written notices were sent to privacy@nike.com over 90 days. Not one produced a reply of any kind, substantive, automated, or a bounce, including to the direct question of whether the mailbox is monitored at all. All six findings stand exactly as originally reported.

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

Disposition

R1 sent 21 June 2026 to privacy@nike.com, bcc the Austrian DSB and CERT.at. Eight further written notices followed through 12 September 2026, cc media.relations@nike.com. No reply of any kind, substantive, automated, or a bounce, was ever received across the entire 90 day window, including to the direct question of whether privacy@nike.com is even a monitored inbox.

ID	Severity	Title
C1	CRITICAL	Hardcoded Firebase and Google Maps API keys in the production APK
C2	CRITICAL	Development and production Airship push credentials hardcoded, inProduction flag left false
H1	HIGH	Forter fraud-scoring SDK: undisclosed cross-merchant fingerprinting and Art. 22 automated decision-making
H2	HIGH	Undisclosed Airship geofencing and Bluetooth beacon detection
H3	HIGH	Singular SDK: cross-app advertising attribution across the Nike app ecosystem

ID	Severity	Title
H4	HIGH	New Relic: HTTP network capture including purchase-flow request details

Subject & Operator Analysis

Nike, Inc. (Beaverton, Oregon) operates its flagship Android application for a global consumer base spanning purchasing, loyalty, and membership functions.

Positive Observations

- android:allowBackup is set to false.
- The network security configuration is clean, using only system certificates with no cleartext domains.
- minSdkVersion 30 is a defensible current baseline.
- No FLEDGE custom-audience permission is requested.

Findings

C1: Hardcoded Firebase and Google Maps API keys 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

A complete Firebase project configuration and a Google Maps key are extracted verbatim from the production binary. The Firebase project name, mynike-prod, confirms it is the live production instance.

```
Firebase API Key: AIzaSyD-xurr4nwsh28hQ5fYRK7sNCtXVERJzpA
Firebase Project:  mynike-prod
Firebase App ID:   1:293647674073:android:9fc2ffe8b7087da1
Storage bucket:    mynike-prod.appspot.com
Google Maps Key:   AIzaSyBJ_ouah7lLkaMkgiZsKfd1Qif052YDzx8
```

No response was received naming this finding. The keys enable probing of the project, reading remote config including pricing, promotion flags, A/B test parameters, feature toggles, and push targeting parameters, accessing Firebase Storage, and, if security rules have gaps, reading user data.

Impact: Publicly extractable production credentials on a global consumer platform enable configuration probing and potential further backend access.

Fix: Rotate both keys, restrict them to the production certificate fingerprint, and confirm the restriction in writing.

C2: Development and production Airship push credentials hardcoded, inProduction flag left false

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

assets/airshipconfig.properties, shipped inside the production Play Store APK, contains both development and production Airship app keys and secrets, with inProduction=false and developmentLogLevel=DEBUG, despite the file's own comment instructing the flag be set to true before app-store submission.

```
developmentAppKey    = QFmpTPAUTbWdyyXw-zKxhQ
developmentAppSecret = HCeKONx1Q4Os2S0jR7GJFA
productionAppKey     = t3Us_93ASi6WRNSaq7Is7g
productionAppSecret  = 8aZZFRH7QIW4u_avrRzU7A
inProduction         = false
developmentLogLevel  = DEBUG

Declared feature set: analytics, contacts, in_app_automation, location, push,
    tags_and_attributes
```

No response was received naming this finding, including three separate yes/no questions asked directly: whether inProduction has been set to true, whether both credentials have been rotated, and whether Airship send logs have been audited for anomalous dispatches since the exposure. Anyone extracting either credential from the APK can send push notifications to Nike's entire subscriber base, stated at potentially hundreds of millions of devices, and read notification analytics and user tags including sneaker preferences, purchase history tiers, geographic targets, and loyalty status.

Impact: A publicly extractable push credential on a platform with a subscriber base in the hundreds of millions enables forged push notifications at scale and exposure of behavioral and loyalty-tier user data.

Fix: Set inProduction to true, rotate both development and production secrets immediately, remove the configuration file from the APK in favor of server-side or Android Keystore delivery, and audit Airship send logs for anomalous dispatches since the exposure.

H1: Forter fraud-scoring SDK: undisclosed cross-merchant fingerprinting and Art. 22 automated decision-making

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

com.forter.mobile.fortersdk.providers.FTRHXContentProvider is present. Forter Inc. (New York) builds cross-merchant device intelligence and behavioral profiles used to score transactions for fraud.

No response was received naming this finding, including RFI-IRFOS's specific framing: 'We are not asserting from static analysis what Forter transmits or how it scores. We are asking what the disclosed basis is.' Forter is not named as a processor in Nike's privacy notice, and purchase decisions potentially affected by an automated fraud score raise Art. 22 automated decision-making questions with no disclosed human-intervention route.

Impact: Purchase-flow decisions may be affected by an undisclosed, cross-merchant automated fraud-scoring system with no confirmed Art. 22(3) human review route.

Fix: Name Forter as an Art. 13(1)(e) processor, disclose its role in automated decision-making, and confirm the Art. 22(3) human-intervention mechanism, or its absence.

H2: Undisclosed Airship geofencing and Bluetooth beacon detection

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 Airship location feature enables geofencing for in-store proximity push targeting; BLUETOOTH and BLUETOOTH_ADMIN permissions support BLE beacon detection.

No response was received naming this finding. This processing activity was not identified as explicitly disclosed under Art. 13(1)(c).

Impact: In-store proximity tracking via geofencing and BLE beacons operates with no confirmed specific user-facing disclosure.

Fix: Disclose the geofencing and BLE beacon detection features and their specific purpose under Art. 13(1)(c).

H3: Singular SDK: cross-app advertising attribution across the Nike app ecosystem

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

190 Singular (San Francisco) smali classes trace Nike ad spend to in-app conversions across the Nike App, SNKRS, and Nike Run Club using advertising identifiers plus Privacy Sandbox Attribution.

No response was received naming this finding.

Impact: Cross-app advertising attribution occurs across Nike's app ecosystem without an identified explicit consent disclosure for this specific data flow.

Fix: Disclose Singular as a named data recipient under Art. 13(1)(e) and its cross-app attribution mechanism specifically.

H4: New Relic: HTTP network capture including purchase-flow request details

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

369 New Relic Inc. (San Francisco) smali classes capture HTTP network interactions including purchase-flow request details, with a RemoteConfiguration class allowing New Relic to adjust instrumentation remotely.

No response was received naming this finding.

Impact: Purchase-flow request details are captured by an undisclosed US application-performance monitoring processor with remotely adjustable instrumentation scope.

Fix: Disclose New Relic as a named data recipient under Art. 13(1)(e) and publish its data-retention and instrumentation-scope policy.

Finding	Provision	Concern

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32	Hardcoded, publicly extractable production credentials
C2	GDPR Art. 32(1), Art. 5(1)(f), Art. 32(2)	Live dev and production push credentials, forged-notification and behavioral-data exposure at scale
H1	GDPR Art. 22, Art. 13(1)(e), Art. 46	Undisclosed cross-merchant automated fraud scoring
H2	GDPR Art. 13(1)(c)	Undisclosed in-store geofencing and BLE beacon detection
H3	GDPR Art. 13(1)(e)	Undisclosed cross-app advertising attribution
H4	GDPR Art. 13(1)(e)	Undisclosed purchase-flow network capture

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to privacy@nike.com, bcc Austrian DSB/CERT.at, 6 findings
2026-06-27 / 06-28	Follow-ups #1-2, cc media.relations@nike.com added, three yes/no questions posed
2026-07-17 / 08-09	Follow-ups #3-4, findings restated, zero reply
2026-08-18	Follow-up #5, day 58, fairness note on positive controls added, weekly SHA-256 re-pull methodology instituted
2026-09-04	Follow-up #6, day 75, deadline lapsed and reset
2026-09-12	Follow-up #7, day 83, direct question of whether privacy@nike.com is even monitored, still unanswered

Date	Event
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Nine written notices across 90 days produced zero replies of any kind, including to the direct question of whether the recipient mailbox is monitored at all. All six findings, including two live push-notification credentials capable of reaching a subscriber base in the hundreds of millions, stand exactly as originally reported.

Residual Risk & Recommendations

- Set inProduction to true and rotate both Airship credentials immediately; this is the single highest-priority item given the scale of the affected subscriber base.
- Rotate the Firebase and Google Maps keys and restrict both to the production certificate fingerprint.
- Name Forter, Singular, and New Relic individually as Art. 13(1)(e) data recipients with their respective processing purposes.
- Disclose the Airship geofencing and BLE beacon detection features specifically.
- Confirm whether privacy@nike.com is a monitored inbox at all, and establish a working reply path independent of it if not.

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, 13, 22, 32, 46. REF NIKE-2026-R1.