Coordinated Security & Privacy Disclosure, Final Report

Strava for Android (com.strava)

Zero certificate pinning on GPS and heart-rate data for 120 million users, a HackerOne redirect, then silence from legal

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY DAYS, ONE REDIRECT, THEN SILENCE

Target	Strava Ireland Limited (lead supervisory authority: Irish DPC)
Product audited	Strava for Android, com.strava, v468.11
Disclosure reference	REF STRAVA-2026-R1
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 Firebase key / C2 zero certificate pinning, 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 Strava Android application and identified six findings, three CRITICAL, three HIGH. The most significant: Strava's network security configuration contains a domain-config entry only for the Android emulator loopback address, 10.0.2.2, and no entry at all for strava.com or any Strava API endpoint, meaning all production traffic for a platform serving roughly 120 million users, GPS track uploads, heart-rate data, segment efforts, and session tokens, is protected only by the Android default certificate store, with zero application-level pinning.

A Firebase API key using a pre-2019 legacy naming convention remains hardcoded and unrotated, suggesting at least seven years of continuous exposure. Separately, allowBackup is set to true with incomplete backup exclusions and no Android 12+ dataExtractionRules, meaning session tokens and cached fitness and chat data are extractable via ADB backup from an unlocked device without root. Three further findings raise undisclosed third-party data flows: a dual ad-attribution pipeline bridging advertising identity to GPS and health data, Embrace SDK workout-session telemetry to an undisclosed US processor, and GetStream chat/video infrastructure, including live call tokens, routed through an undisclosed US sub-processor.

Strava Security's only substantive reply, one day after R1, redirected the disclosure to its HackerOne bug bounty program. RFI-IRFOS declined the redirect the same day and escalated to Strava's legal department. No reply of any kind was received from legal, security, or the original responding engineer across five further written notices and 90 days.

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

Disposition

R1 sent 21 June 2026 to security@strava.com, bcc the Austrian DSB, CERT.at, and the Irish DPC. Strava Security redirected the disclosure to its HackerOne bug bounty program the next day. RFI-IRFOS declined and escalated to legal@strava.com the same day. Five further written notices followed through 11 September 2026. No reply of any kind was received from legal, security, or the original responding engineer after that single redirect.

ID	Severity	Title
C1	CRITICAL	Hardcoded Firebase API key, legacy naming convention, at least seven years unrotated
C2	CRITICAL	Zero certificate pinning on production traffic for a platform serving roughly 120 million users
C3	CRITICAL	allowBackup enabled with incomplete exclusions, no Android 12+ dataExtractionRules
H1	HIGH	Undisclosed dual ad-attribution pipeline bridging advertising identity to GPS and health data

ID	Severity	Title
H2	HIGH	Embrace SDK: workout-session telemetry to an undisclosed US processor
H3	HIGH	GetStream.io: club chat and live video call tokens through an undisclosed US sub-processor

Subject & Operator Analysis

Strava Ireland Limited operates the Strava GPS and fitness-tracking platform for a global userbase reported in the hundreds of millions, with the Irish DPC as lead supervisory authority.

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, legacy naming convention, at least seven years unrotated

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 AIzaSyDoncveJ-bM9--2J9ODDC8GKQ9H6lUGXXk, project api-project-541588808765, a naming scheme Google retired around 2019, extracted from res/values/strings.xml.

```
API Key:  AIzaSyDoncveJ-bM9--2J9ODDC8GKQ9H6lUGXXk
Project:  api-project-541588808765
DB URL:   https://api-project-541588808765.firebaseio.com
App ID:   1:541588808765:android:29df5cf9440ac761
```

No response was received naming this finding. The legacy naming convention alone suggests continuous production use for at least seven years without rotation, enabling probing of the Firebase database, forged push notifications, and remote-config enumeration.

Impact: A credential extractable from any downloaded APK, unrotated for at least seven years, enables FCM probing and potential further backend access.

Fix: Rotate the credential, restrict it to the production certificate fingerprint, and confirm the rotation in writing.

C2: Zero certificate pinning on production traffic for a platform serving roughly 120 million users

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 contains a domain-config entry only for the Android emulator loopback address, 10.0.2.2. No domain-config entry and no pin-set exist anywhere in the file for strava.com, *.strava.com, or any Strava API endpoint.

```
<debug-overrides>...</debug-overrides>  <- debug builds only, correctly scoped
<domain-config cleartextTrafficPermitted="true">
  <domain>10.0.2.2</domain>            <- Android emulator loopback ONLY
</domain-config>

<!-- No domain-config or pin-set exists for strava.com or *.strava.com anywhere in the
     file -->
```

No response was received naming this finding. GPS track uploads, heart-rate data, segment efforts, and session tokens for approximately 120 million users are protected only by the Android default system certificate store, interceptable in transit by any actor holding a system-trusted CA, including a rogue Wi-Fi access point, enterprise MDM, or a compromised CA. RFI-IRFOS cited Strava's 2018 global heatmap incident, in which aggregated GPS data publicly exposed military installation locations, as evidence that this GPS data surface is a national-security-relevant asset, not merely a consumer privacy matter.

Impact: All production traffic, including precise GPS location history for a userbase in the hundreds of millions, is exposed to interception on any network where a trusted-but-hostile certificate authority is present.

Fix: Add domain-config entries for strava.com and *.strava.com with SHA-256 certificate pins and cleartextTrafficPermitted set to false.

C3: allowBackup enabled with incomplete exclusions, no Android 12+ dataExtraction-Rules

MEDIUM, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1

android:allowBackup="true" with a backup scheme excluding only the main database and two named shared-preference files. Other databases (route cache, chat history, telemetry cache) and all other shared preferences are not excluded, and no android:dataExtractionRules is present for Android 12 and later.

No response was received naming this finding. Physical access to an unlocked device allows extraction of session tokens, fitness cache, and chat history via adb backup, without root, since Android 12+ cloud backup falls through to system defaults for all non-excluded data.

Impact: An unlocked device in an attacker's physical possession can have session tokens and cached fitness and chat data extracted without root access.

Fix: Add comprehensive android:dataExtractionRules exclusions for Android 12 and later, or set android:allowBackup to false.

H1: Undisclosed dual ad-attribution pipeline bridging advertising identity to GPS and health data

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

ACCESS_ADSERVICES_ATTRIBUTION, ACCESS_ADSERVICES_AD_ID, and a separate Branch.io attribution pipeline together bridge ad click-through identity to a user's Strava profile, GPS routes, heart-rate history, segment efforts, and club memberships.

No response was received naming this finding. This processing purpose, linking advertising identity to health and location data, is not disclosed in Strava's privacy policy.

Impact: Advertising identity is linked to GPS route and heart-rate history through two parallel, undisclosed attribution pipelines.

Fix: Disclose the ad-attribution to fitness-data bridge explicitly under Art. 13, and confirm the Art. 6(1) legal basis.

H2: Embrace SDK: workout-session telemetry to an undisclosed US processor

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

138 Embrace Mobile Inc. (San Francisco) smali classes record app sessions, crashes, user flows, and network request metadata tied directly to workout sessions, transmitted to Embrace's US infrastructure.

No response was received naming this finding. Embrace Inc. is not named as a data processor in Strava's privacy policy, and no Art. 46 transfer mechanism is documented.

Impact: Behavioral context tied to workout sessions is transmitted to an undisclosed US processor with no documented transfer safeguard.

Fix: Name Embrace Inc. as a processor under Art. 13(1)(e) and publish its Art. 46 transfer mechanism.

H3: GetStream.io: club chat and live video call tokens through an undisclosed US sub-processor

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 io.getstream.chat SDK routes club chat through GetStream's US servers and includes a live video call token API.

No response was received naming this finding. GetStream Inc. is not named as a sub-processor in Strava's privacy policy.

Impact: Club messages and video call session tokens are routed through an undisclosed US sub-processor with no documented transfer safeguard.

Fix: Name GetStream Inc. as a sub-processor under Art. 13(1)(e) and publish its Art. 46 transfer mechanism.

Strava's Response, Recorded in Full

On 22 June 2026, the day after R1, Kelly ("Kosta") Kaoudis of Strava Security replied, in full: "Thank you for reaching out to us. We currently only accept vulnerability/bug bounty reports through HackerOne. So that we can add this report to our triage queue and evaluate it for potential reward, please split your bulk report into individual potential findings, and email them to vulnerabilities@strava.com... Note that to submit a vulnerability report via HackerOne, you will need to create a HackerOne account if you do not already have one."

RFI-IRFOS declined the redirect the same day, stating this is a formal GDPR security and privacy disclosure, not a bug report, and escalated to legal@strava.com. A full restatement was sent on 28 June, naming the pattern as a VDP Redirect and posing three specific yes/no questions on credential awareness, certificate-pinning status, and remediation timing relative to regulator contact. None of the three questions, and no further message from legal, security, or Kosta Kaoudis, was ever answered across five subsequent written notices through 11 September 2026.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(2)	Hardcoded, unrotated credential, at least seven years old
C2	GDPR Art. 32(1)(a), Art. 25	Zero certificate pinning on all production traffic
C3	GDPR Art. 32, Art. 25	Incomplete backup exclusions, ADB-extractable session data
H1	GDPR Art. 5(1)(c), Art. 13, Art. 6(1)	Undisclosed ad-identity to health-data bridge
H2	GDPR Art. 13(1)(e), Art. 46	Undisclosed US telemetry processor
H3	GDPR Art. 13(1)(e), Art. 46	Undisclosed US chat/video sub-processor

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to security@strava.com, bcc Austrian DSB/CERT.at/Irish DPC, 6 findings
2026-06-22	Kosta Kaoudis (Strava Security) redirects to HackerOne; RFI-IRFOS declines same day and escalates to legal@strava.com
2026-06-28	Full restatement to legal, VDP Redirect pattern named, three yes/no questions posed
2026-07-23 / 08-09 / 08-15	Follow-ups; Austrian DSB and Irish DPC moved from bcc to visible cc
2026-09-03 / 09-11	Final follow-ups restate all findings; weekly SHA-256 re-pull instituted
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Strava's only substantive reply, received one day after R1, was a bug-bounty redirect. After RFI-IRFOS declined and escalated to legal, no reply of any kind was received from legal, security, or the original responding engineer across five further written notices and 90 days.

Residual Risk & Recommendations

- Add certificate pinning for strava.com and *.strava.com; this is the single highest-priority item given the GPS and health-data exposure across the platform's full userbase.
- Rotate the seven-year-old Firebase credential and restrict it to the production certificate fingerprint.
- Add comprehensive Android 12+ dataExtractionRules exclusions or disable allowBackup entirely.
- Disclose the ad-attribution to health-data bridge, and name Embrace Inc. and GetStream Inc. as processors with their respective transfer mechanisms.
- Confirm whether legal@strava.com is a monitored inbox at all, given zero reply across five written notices and 82 days since escalation.

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, 32, 46. REF STRAVA-2026-R1.