Coordinated Privacy Disclosure, Final Report

Coca-Cola CEE (com.cocacola.app.cee)

The Coca-Cola Company, CEE loyalty platform (win.coke.at); bottling and EU operating partner Coca-Cola HBC AG

SILENT · CASE CLOSED AND PUBLISHED 24 SEPTEMBER 2026, 96 DAYS AFTER DISCLOSURE, FIVE MESSAGES SENT, ZERO REPLY OF ANY KIND

Target	Coca-Cola CEE, a consumer loyalty and promotions app for Central and Eastern Europe (win.coke.at)
Package	com.cocacola.app.cee
Operator	The Coca-Cola Company; bottling and EU operating partner Coca-Cola HBC AG
Initial Disclosure	2026-06-20
Original Embargo	2026-09-19 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-24, five days after the embargo, an internal publishing gap, not a change in terms
Regulators in BCC	Austrian DSB, CERT.at
Total Outbound Messages	5, across 96 days, to DPO-Europe@coca-cola.com. A separate initial attempt to privacy@coca-cola.com and datenschutz@coca-cola.at on 28 June 2026 bounced three times and was abandoned in favor of the DPO-Europe address.
Inbound Replies	0. No reply, automated or human, was ever received at DPO-Europe@coca-cola.com.

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 disclosed to The Coca-Cola Company that its Central and Eastern Europe loyalty app, Coca-Cola CEE, ships a hardcoded Firebase credential, a memory heap debugger (LeakCanary) that should never reach a consumer release, and an Adobe Experience Platform Assurance WebSocket bridge that, when activated by scanning a QR code, can stream a user's live analytics events, prize interactions, code scans, game plays, and location, to an external monitoring console whose target address is itself configurable via the same QR code mechanism.

Four further findings describe an attribution and behavioral-tracking architecture disproportionate to a prize-administration app: Storyly (App Samurai, Istanbul and the US) tracking every promotional story view and swipe; AppsFlyer building a complete bottle-scan-to-prize attribution funnel on US infrastructure; a second, OS-level attribution pipeline running in parallel via Android's Privacy Sandbox; and a production APK that still bundles a Charles proxy development certificate. A final finding names a specific internal contradiction: the app ships gambling-adjacent mechanics, scratch cards, raffles, loot chests, and shake-to-win, alongside an animation file named specifically for an age check, confirming the operator's own awareness that age-gating is required, while providing no functional verification of age at all.

Five messages were sent to DPO-Europe@coca-cola.com, cc'ing DataProtectionOffice@cchellenic.com and press@coca-cola.com, and bcc'ing the Austrian DSB and CERT.at, across 96 days. A separate initial attempt on 28 June 2026 to privacy@coca-cola.com and datenschutz@coca-cola.at bounced three times and was abandoned in favor of the DPO-Europe channel, which itself never once replied. The 90-day embargo, set at first contact, elapsed on 19 September 2026. This report and the accompanying closure notice publish five days later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production Coca-Cola CEE Android application (com.cocacola.app.cee, version 2.202.2, versionCode 40202, 33,220 smali classes across 4 DEX files), covering the AndroidManifest, resource strings, decompiled dex/smali, and bundled assets, as pulled and reviewed on 20 June 2026. No dynamic instrumentation, live traffic capture, QR-code activation of the Adobe Assurance bridge, or interaction with Coca-Cola's backend infrastructure was performed.

Disposition

Eight findings were disclosed on 20 June 2026, later re-scored under CVSS v4.0: one finding independently reaches HIGH on the computed CVSS score alone, without any editorial escalation (an Adobe Experience Platform Assurance WebSocket bridge, activatable via QR code scan, capable of streaming live analytics events, including prize interactions and location data, to an external console). A hardcoded Firebase key and three further findings correct down to MEDIUM. A production heap-dump debugger corrects down to LOW. Two findings, gambling-adjacent game mechanics paired with a cosmetic-only age-check animation, and a bundled development proxy certificate, are classified OBSERVATIONAL, real and worth recording but not demonstrated technical attack paths on their own. Five messages were sent across 96 days. Not one reply of any kind was ever received.

ID	Severity	Title
C1	MEDIUM	Firebase API Key Hardcoded in the Distributed Binary
H1	LOW	LeakCanary Memory Heap Debugger Present in the Production Release
H2	HIGH	Adobe Experience Platform Assurance WebSocket Bridge, Activatable by Scanning a QR Code, Can Stream Live Analytics Events to an External Console
H3	MEDIUM	Storyly Promotional Story Tracking, 675 Classes, Not Disclosed as a Data Recipient
H4	MEDIUM	AppsFlyer, 448 Classes, a Full Bottle-Scan-to-Prize Attribution Funnel Routed to US Infrastructure
H5	MEDIUM	A Second, OS-Level Attribution Pipeline Runs in Parallel via Android's Privacy Sandbox
H6	OBSERVATIONAL	Gambling-Adjacent Game Mechanics Ship Alongside a Cosmetic, Non-Functional Age Check
H7	OBSERVATIONAL	A Charles Proxy Development Certificate Is Bundled in the Production APK

Subject & Operator Analysis

Coca-Cola CEE (com.cocacola.app.cee) is a consumer loyalty and promotions platform for Central and Eastern Europe, operated by The Coca-Cola Company with Coca-Cola HBC AG as the EU bottling and operating partner. Users scan bottle-cap barcodes and NFC caps, enter prize codes, and play promotional mini-games to redeem prizes.

Several genuine positives are worth naming up front. Certificate pinning on both production API endpoints is correctly implemented with SHA-256 pins valid through 2030. minSdk 29 (Android 10) is the highest minimum SDK RFI-IRFOS has observed in this audit series, materially reducing unpatched-OS exposure. Passkey authentication via Microsoft MSAL WebAuthn is genuinely uncommon and a real investment in a consumer loyalty app. Google reCAPTCHA for sweepstakes bot prevention and ML Kit/ZXing barcode scanning proportionate to the CAMERA permission are both sound engineering choices. The issues documented here sit in what shipped alongside that foundation, not in the foundation itself.

Architecture & Data Flow

A single bottle-cap scan and prize claim passes through at least four independent data pipelines: LeakCanary's local heap monitoring (H1), Storyly's promotional-engagement tracking (H3), AppsFlyer's attribution funnel (H4), and the Android Privacy Sandbox's parallel OS-level attribution API (H5), none individually named as a data recipient in the privacy documentation. A hardcoded Firebase key (C1) sits beneath all of it at the operational-security layer, and a QR-code-activatable Adobe Assurance WebSocket bridge (H2) provides a live event-streaming path, a genuine technical attack surface, not merely an undisclosed-recipient question, distinct from the others.

Findings

C1: Firebase API Key Hardcoded in the Distributed Binary

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

The Firebase API key, database URL, and app ID for the coca-cola-prod project are present verbatim in res/values/strings.xml, extractable from the public APK in under 60 seconds. Firebase keys are not secrets by design, so this finding is about availability, not confidentiality: a party holding the key can exhaust the project's Firebase quota, affecting Analytics, Crashlytics, Messaging, Performance Monitoring, Remote Config, and A/B Testing simultaneously.

```
res/values/strings.xml
google_api_key:          AIzaSyB3atwNbq7s5PJIF5sbxrTHXXMFuNCu_ZY
firebase_database_url:   https://coca-cola-prod.firebaseio.com
google_app_id:           1:670511801438:android:26942dd992e4177b
default_web_client_id:   670511801438-qlkhsnrsmfqlaa5ab80c1jl0gjs95618.apps.
    googleusercontent.com
Firebase modules active: Analytics, Crashlytics, Messaging, Performance, Remote Config
    , A/B Testing
```

Impact: Quota exhaustion or credential abuse can disrupt Analytics, Crashlytics, Messaging, Remote Config, and A/B Testing simultaneously for a loyalty platform serving multiple CEE markets.

Fix: Rotate the exposed key, apply Firebase App Check and key restrictions, and route configuration and messaging through an authenticated backend layer. No confirmation that this has occurred was ever received.

H1: LeakCanary Memory Heap Debugger Present in the Production Release

LOW, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.4.

LeakCanary (25 smali classes), a development-only memory-leak detection library, is present in the production APK, not its no-op release stub. At runtime the JVM heap it monitors can contain active session tokens, prize codes, personal data loaded from the backend, and in-transit location data. Exploiting this requires access to the device or its local storage, which is why this corrects down from the original HIGH label; it remains a real development-hygiene gap worth fixing.

```
smali/leakcanary/internal/*.smali -- 25 classes present in release build
# should be declared testImplementation or the no-op stub in release:
# implementation 'com.squareup.leakcanary:leakcanary-android-no-op:...'
```

Impact: A party with local device access, physical possession, malware, or a backup extraction, could recover session tokens, prize codes, and personal data from a heap dump the app itself was never meant to generate outside development.

Fix: Replace LeakCanary with its no-op stub in the release build configuration. No confirmation that this has occurred was ever received.

H2: Adobe Experience Platform Assurance WebSocket Bridge, Activatable by Scanning a QR Code, Can Stream Live Analytics Events to an External Console

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 7.1. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

assets/WebviewSocket.html is the Adobe Experience Platform Assurance (formerly Griffon) real-time monitoring bridge, a development and QA tool that remains active in the consumer release. Once triggered by scanning a QR code, it opens a WebSocket connection and streams all Adobe SDK analytics events live, including prize interactions, code scans, game plays, and location events, to whichever console the connection targets. Because the WebSocket target URL is itself set by the QR code that activates the flow, a user who scans a maliciously crafted QR code, not one supplied by Coca-Cola, could have their live event stream redirected to a third party's console, not Adobe's own.

```
assets/WebviewSocket.html (Adobe copyright 2022)
function connect(url) {
    nativeCode.log("Socket is connecting to: " + url);
    _socket = new WebSocket(url);
    _pingInterval = setInterval(doPing, PING_INTERVAL_IN_MS);
# target url is QR-code-supplied, not hardcoded to an Adobe-controlled endpoint
```

Impact: A user who scans an unofficial QR code, plausible in a promotional context built around barcode and NFC-cap scanning, could have their live purchase, location, and game-interaction event stream redirected to a monitoring console outside Coca-Cola's or Adobe's control.

Fix: Strip the Adobe Assurance WebSocket bridge from production builds entirely; a QA tool with a user-triggerable, externally-addressable activation path has no place in a consumer release. No confirmation that this has occurred was ever received.

H3: Storyly Promotional Story Tracking, 675 Classes, Not Disclosed as a Data Recipient

---

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.

Storyly (App Samurai, Istanbul, with US operations, 675 smali classes) captures which promotional story a user viewed, dwell time, swipe behavior, and CTA taps, an engagement profile of which prizes and brands interest a given user. No transfer mechanism for this data to Turkey or the US is disclosed at the app level.

```
com/appsamurai/storyly/                -- core SDK, 675 classes
com/appsamurai/storyly/analytics/      -- event tracking
"storylyTracker" / "onSwipe(ReelsTouchHandler$Action)" -- confirmed active in
    production
```

Impact: A behavioral profile of which promotions and brands engage a given user is built and transmitted to a Turkish/US vendor with no disclosed legal basis or transfer mechanism.

Fix: Name App Samurai/Storyly individually as a data recipient with a stated Art. 44-49 transfer mechanism in the privacy documentation. No confirmation that this has occurred was ever received.

H4: AppsFlyer, 448 Classes, a Full Bottle-Scan-to-Prize Attribution Funnel Routed to US Infrastructure

---

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.

AppsFlyer (448 smali classes, US-headquartered) connects acquisition source to in-app events, code scans, prize claims, game plays, building a commercial profile of which promotions a user responds to and which redemptions convert them to further purchases. This scope of profiling exceeds what prize administration itself requires, and no transfer mechanism to US infrastructure is disclosed.

Impact: Purchase and engagement behavior tied to a specific bottle scan is profiled and transmitted to US infrastructure for commercial attribution purposes distinct from, and not disclosed alongside, prize administration.

Fix: Name AppsFlyer individually as a data processor with a stated legal basis and transfer mechanism under Art. 13(1)(e) and Art. 44-49. No confirmation that this has occurred was ever received.

H5: A Second, OS-Level Attribution Pipeline Runs in Parallel via Android's Privacy Sandbox

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.

ACCESS_ADSERVICES_ATTRIBUTION and ACCESS_ADSERVICES_AD_ID register purchase-code scans and game interactions as attribution events directly with the Android OS, independent of and in addition to the AppsFlyer SDK layer (H4). Two simultaneous, independent attribution pipelines exceed what is necessary for prize administration, and neither pipeline's purpose is stated with a legal basis in the privacy documentation.

```
android.permission.ACCESS_ADSERVICES_ATTRIBUTION
android.permission.ACCESS_ADSERVICES_AD_ID
com.google.android.gms.permission.AD_ID
```

Impact: Conversion events are captured twice, once by AppsFlyer's SDK and once by the OS-level Privacy Sandbox API, doubling the attribution surface with no individually disclosed purpose for either.

Fix: Document a specific Art. 6(1) legal basis and Art. 13(1)(c) disclosure for the Privacy Sandbox Attribution pipeline distinct from the AppsFlyer SDK. No confirmation that this has occurred was ever received.

H6: Gambling-Adjacent Game Mechanics Ship Alongside a Cosmetic, Non-Functional Age Check

OBSERVATIONAL — not independently CVSS-scored; a consumer-protection and regulatory-compliance question, not a demonstrated technical attack path.

Production assets confirm a complete chance-based promotional toolkit: scratch cards, raffles, loot chests, shake-to-win, and multiple branded mini-games with random prize outcomes. An underage_animation.json file confirms the app's own developers recognized that age-gating is required for this content; what exists is an animation, not a verified age-check mechanism. Under the Austrian Glücksspielgesetz and the EU Digital Services Act's age-assurance provisions, operators of chance-based prize mechanics are expected to implement effective, not cosmetic, age controls.

```
assets/ (Lottie animation files, confirmed in production APK)
scratch.json, raffle_button_animation.json, chest_animation.json,
phone_shake_animation.json, game_fanta.json, game_push_the_button.json,
game_xmas.json, underage_animation.json -- present, animation only
```

Impact: The app's own asset naming demonstrates awareness that its randomized-prize mechanics require age-gating, while the mechanism actually shipped provides no functional verification of a user's age.

Fix: Replace the cosmetic age-check animation with an effective age-assurance mechanism proportionate to Austrian GSpG and EU DSA Art. 28 requirements. No confirmation that this has occurred was ever received.

H7: A Charles Proxy Development Certificate Is Bundled in the Production APK

OBSERVATIONAL — not independently CVSS-scored; debug-overrides referencing this certificate are inactive in release builds, so this is a development-hygiene artifact, not an active trust-anchor risk to users.

res/raw/charles_certificate, a commercial HTTP(S) inspection proxy certificate, is bundled in the production APK and referenced from the manifest's debug-overrides trust-anchor configuration. Android ignores debug-overrides in a non-debuggable release build, so the certificate does not grant any party a working trust anchor on end-user devices. It remains extractable from the APK, revealing that Charles proxy was used to inspect the app's traffic to cca-api.coca-cola.com and AWS AppSync during development, a hygiene gap in the release-build packaging process, not a live risk to users.

Impact: No functional risk to end users given inactive debug-overrides in release builds; the finding is stated purely as a development-process hygiene gap worth closing before the next release.

Fix: Strip development-only certificates and debug-overrides configuration from the production build entirely. No confirmation that this has occurred was ever received.

Impact Analysis

H2 stands apart from the other findings in kind, not just severity: H1, H3, H4, and H5 describe undisclosed or improperly-packaged data flows, real gaps, but not exploitable in the traditional sense. H2 describes an active technical attack surface instead, a QR-code-triggered WebSocket whose target address a malicious QR code could redirect, reaching a computed CVSS v4.0 score of HIGH on its own. It is the one finding in this report where RFI-IRFOS recommends treating the fix as time-sensitive, not a documentation gap to close at the next release cycle.

Five Messages, 96 Days, Zero Reply

This case's correspondence record is total silence. Five messages were sent to DPO-Europe@coca-cola.com across 96 days, cc'ing DataProtectionOffice@cchellenic.com and press@coca-cola.com, and bcc'ing the Austrian DSB and CERT.at throughout. A separate initial attempt on 28 June 2026 to privacy@coca-cola.com and datenschutz@coca-cola.at bounced three times in a row and was abandoned in favor of the DPO-Europe channel. Not one reply, automated or human, was ever received at either address.

Article	Finding	Basis

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 32(1)(b), Art. 13(1)(e)	C1	Hardcoded Firebase credential, availability risk across six active Firebase modules.
Art. 32(1)(b), Art. 25(1)	H1	Production-release heap debugger exposing session tokens and personal data to local access.
Art. 32(1)(b), Art. 5(1)(f)	H2	QR-code-activatable, externally-addressable live event-streaming bridge, undisclosed.
Art. 13(1)(e), Art. 44-49	H3	Undisclosed promotional-engagement tracking recipient, no stated transfer mechanism.
Art. 13(1)(e), Art. 6(1)(f)	H4	Undisclosed attribution profiling recipient, purpose distinct from prize administration.
Art. 13(1)(c), Art. 6(1)	H5	Second, parallel OS-level attribution pipeline, no individually stated legal basis.

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 CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. In this report, H2 reaches HIGH on its computed CVSS v4.0 score alone, with no editorial escalation applied or needed; C1, H3, H4, and H5 correct down to MEDIUM and H1 corrects down to LOW to match their own computed bands; H6 and H7 are classified OBSERVATIONAL because they are real, transparency-relevant findings without a demonstrated technical attack path to score. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungs-

freiheitsgesetz, Art. 17 StGG. REF REF: com.cocacola.app.cee.