Coordinated Security & Privacy Disclosure, Final Report

ChessKid (com.chesskid)

Chess.com LLC, operated via Chessable Spain S.L. (EEA representative) and Chessable Ltd (UK representative)

SILENT · CASE CLOSED AND PUBLISHED 23 SEPTEMBER 2026, 91 DAYS AFTER DISCLOSURE, ZERO SUBSTANTIVE REPLY EVER RECEIVED

Target	ChessKid, an online chess platform and companion app for children, operated by Chess.com LLC
Package	com.chesskid, version 3.2.2 at time of original disclosure
Operator	Chess.com LLC (US). EEA representative: Chessable Spain S.L., Barcelona. UK representative: Chessable Ltd, London.
Initial Disclosure	2026-06-24
Original Embargo	2026-09-22 (90 days from disclosure)
Case Closed	2026-09-23, one day after the embargo, once no substantive reply had arrived
Regulators in BCC	Austrian DSB, German BfDI, UK ICO
Total Outbound Messages	11, across 91 days
Inbound Messages	10, all automated acknowledgments (press and DPO auto-reply mailboxes). Zero human-authored replies at any point.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 24 June 2026, RFI-IRFOS disclosed to Chess.com that ChessKid, a chess platform marketed to and used by children, ships a hardcoded Amplitude analytics API key in its production Android binary. The key is a live credential, not a project identifier, and grants an external party full read and write access to the behavioural analytics dataset Amplitude holds for ChessKid's users: exporting event histories, reading user properties, identifying cohorts, and injecting fabricated events into the pipeline. RFI-IRFOS also disclosed a hardcoded Firebase API key and the absence of any disclosed lawful basis or parental consent mechanism for the Amplitude analytics processing itself.

Across 91 days and eleven outbound messages to Chess.com's press and DPO contact addresses, RFI-IRFOS received ten automated acknowledgments and zero human-authored replies. No finding was disputed. No finding was confirmed as fixed. No question, including the three yes-or-no questions in the original disclosure, was ever answered.

This report closes the case on the terms stated in the original message: coordinated disclosure with a fixed 90-day period, publication on schedule regardless of engagement. RFI-IRFOS re-scored all three findings under CVSS v4.0 for this report, not carrying forward the original hand-assigned severities unchanged. The Amplitude key finding (C1) scores CRITICAL, 9.3, consistent with the original label. The Firebase key finding, originally labeled HIGH, scores MEDIUM, 6.9, under a proper CVSS v4.0 derivation and is corrected accordingly in this report. The undisclosed children's-data analytics finding, originally labeled HIGH, has a CVSS v4.0 base score of MEDIUM, 6.9, and is held at HIGH in this report under an explicit blast-radius escalation, documented in the finding itself, because the affected population is children under the age threshold GDPR Art. 8 and COPPA both exist to protect.

Scope: Root-level static analysis of the production ChessKid Android application (com.chesskid, version 3.2.2), covering the AndroidManifest, resource strings, and the app's own published privacy policy, as pulled and reviewed on 24 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Chess.com's backend infrastructure was performed. RFI-IRFOS was unable to pull a fresh production build for this closure report; the weekly-diff monitoring this campaign otherwise performs against an archived binary did not run for this case in the environment available at closure, and this report does not claim to know whether the three findings still hold against the current Google Play build. That gap is stated here explicitly, it is not left implicit.

Disposition

Three findings were disclosed on 24 June 2026: a hardcoded Amplitude analytics API key granting full read and write access to children's behavioural data (C1), a hardcoded Firebase API key (originally labeled H1), and undisclosed Amplitude analytics processing of children's behavioural data without a stated lawful basis or parental consent framework (originally labeled H2). Eleven messages were sent across 91 days to Chess.com's press and DPO contact channels. Every one of the ten inbound messages received in return was an automated acknowledgment, never a human reply. No fix was ever confirmed, no denial was ever issued, no question was ever answered. This report closes and publishes the case as scheduled, on the terms disclosed from the first message: a fixed coordinated-disclosure period, independent of engagement.

ID	Severity	Title
C1	CRITICAL	Hardcoded Amplitude API Key, Full Read/Write on Children's Behavioural Data
H1	MEDIUM	Hardcoded Firebase API Key, Severity Corrected From the Original Disclosure
H2	HIGH	Undisclosed Children's Behavioural Analytics, No Stated Lawful Basis, No Parental Consent Framework

Subject & Operator Analysis

ChessKid is a chess platform and companion Android application marketed to and used by children, operated by Chess.com LLC (United States). Chess.com designates Chessable Spain S.L. (Barcelona) as its EEA representative and Chessable Ltd (London) as its UK representative, both named in ChessKid's own published policies at the time of disclosure. Chess.com maintains dedicated press and DPO contact mailboxes (press@chess.com, dpo@chess.com), both of which returned automated acknowledgments throughout this case and never a human reply.

ChessKid's own child-safety product features, content moderation, chat filters, a parental dashboard, and age-appropriate UX, are real and are not the subject of this report. The findings here sit in the credential-management layer of the binary and in the undisclosed analytics processing running alongside those child-safety features, not in the features themselves.

Architecture & Data Flow

The ChessKid production APK (version 3.2.2 at time of disclosure) compiles two hardcoded third-party credentials directly into the distributed binary: an Amplitude analytics API key and a Firebase API key, both extractable from res/values/strings.xml with no specialist tooling. The Amplitude key sits in front of a behavioural analytics pipeline that receives session data, feature interactions, game outcomes, and user progression events for every ChessKid user, including the platform's core child user base, and that pipeline is never named as a data recipient in ChessKid's own privacy policy.

Findings

C1: Hardcoded Amplitude API Key, Full Read/Write on Children's Behavioural Data

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.

res/values/strings.xml in the ChessKid production APK contains a hardcoded Amplitude analytics API key (amplitude_api_key = 89e2a8ad36ed610a5b68c94e3ccf4412). This is a live server-side credential, not a public project identifier: it authorizes read access to Amplitude's user-search and export endpoints and write access to Amplitude's event-ingestion endpoint for ChessKid's project. The adjacent amplitude_api_key_dev field in the same file is empty, meaning Chess.com's own codebase distinguishes a development key from a production key, and the production key was compiled into the distributed binary regardless.

```
res/values/strings.xml:
<string name="amplitude_api_key">89e2a8ad36ed610a5b68c94e3ccf4412</string>
<string name="amplitude_api_key_dev"></string>
```

Extraction requires no specialist tooling: apktool d chesskid.apk, then grep amplitude_api_key against the extracted resource strings. With the key in hand, an external party can query Amplitude's /2/usersearch endpoint to export user event histories and properties, identify user cohorts and segments, and post fabricated events to /2/httpapi, all against a dataset generated by children learning to play chess, some as young as six.

This finding was never disputed by Chess.com at any point across the correspondence. No message from any Chess.com address addressed C1 specifically, in either direction, substantive or automated.

Impact: Full read access to a children's behavioural analytics dataset, and full write access to inject fabricated events into that same dataset, both without Chess.com's own authorization boundary being involved at all. Because the key is compiled into every copy of the distributed APK, the exposure is not limited to a single account or session, it is the same static credential shipped to every installation.

Fix: Rotate the exposed Amplitude key immediately and move analytics event ingestion behind a server-side proxy that authenticates the requesting client without embedding the Amplitude project credential in the distributed binary. No confirmation that this has occurred was ever received.

H1: Hardcoded Firebase API Key, Severity Corrected From the Original Disclosure

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. Originally labeled HIGH in the 24 June 2026 disclosure.

res/values/strings.xml also contains a hardcoded Firebase API key (google_api_key and google_crash_reporting_api_key, both AIzaSyDj5RBLsTR_p5mZiJtMUim0tT1LFqyuNBs) . No exposed Firebase Realtime Database URL, no confirmed open security rules, and no other demonstrated exploitation path was ever identified for this specific credential, a materially narrower exposure than the Amplitude key. Google's own documentation states Firebase API keys of this kind are public-by-design project identifiers, not access secrets in themselves.

Severity correction, made in this report: the original 24 June 2026 disclosure labeled this finding HIGH without a CVSS derivation. Scored properly under CVSS v4.0 against only what was actually demonstrated, an exposed project-identification key with no confirmed downstream exposure, the finding lands at MEDIUM, 6.9. The residual risk is availability-oriented, quota exhaustion against the associated Firebase project by a party using the exposed key, not confidentiality or integrity of user data. This report carries the corrected severity, not the original label, per RFI-IRFOS's own severity-consistency discipline.

Impact: A third party in possession of this key can attribute requests to Chess.com's Firebase project and, depending on the project's own quota and rule configuration (neither confirmed by RFI-IRFOS), potentially exhaust API quota. No confirmed access to user data was ever demonstrated for this specific finding.

Fix: Apply standard Firebase API key restrictions, package name and signing certificate binding at minimum, per Google's own published guidance for exactly this class of key. No confirmation that this has occurred was ever received.

H2: Undisclosed Children's Behavioural Analytics, No Stated Lawful Basis, No Parental Consent Framework

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. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the affected population is children under the age threshold GDPR Art. 8 and COPPA exist specifically to protect, and the processing was never disclosed to a parent or guardian at all.

ChessKid integrates Amplitude behavioural analytics, session data, feature interaction, game outcomes, and user progression, on a platform explicitly marketed to children. At the time of the original disclosure, ChessKid's published privacy policy did not name Amplitude as a data processor, did not state a lawful basis for this specific analytics processing, and did not describe a parental consent mechanism covering it. GDPR Art. 13 requires naming recipients or categories of recipients; Art. 8 requires parental consent for processing a child's personal data below the relevant national age threshold; COPPA imposes an equivalent requirement in the United States.

This is a disclosure and legal-basis gap, not a code-level exploit, and CVSS's own base metrics understate it for exactly that reason, the framework is built to score technical attack paths, not the absence of a required legal basis for processing a protected population's data. RFI-IRFOS applies its own blast-radius escalation for this class of finding, documented here

explicitly per RFI-IRFOS's own severity-consistency discipline, the CVSS number itself is not silently inflated.

Impact: Ongoing behavioural profiling of children, through a named third-party processor never disclosed to a parent or guardian, with no lawful basis stated anywhere ChessKid's users or their parents could have found it before installing or using the app.

Fix: Disclose Amplitude by name as a data processor, state the specific lawful basis relied on for this processing, and implement or document a parental consent mechanism covering it specifically, not folded into a general terms-of-service acceptance. No confirmation that any of this has occurred was ever received.

Impact Analysis

The practical impact of these three findings compounds, the three do not sit side by side as isolated issues. The Amplitude key (C1) is not just a credential-hygiene lapse, it is the access mechanism into a behavioural dataset that H2 establishes was never disclosed, never given a stated lawful basis, and never covered by parental consent in the first place. A dataset that should not exist in its current disclosed form is also a dataset that, per C1, anyone with the APK can read in full and write fabricated events into.

The Complete Chain

A user installs ChessKid, a platform marketed to children. The app begins sending session, fe ature-interaction, and progression events to Amplitude under a production API key compiled into every copy of the binary. No parent-facing disclosure names Amplitude or states a lawful basis for this specific processing. Separately, the same production API key, extractable by anyone with the public Play Store build, grants full read access to the resulting dataset and full write access to inject fabricated events into it. Ninety-one days and eleven messages later, no part of this chain had been confirmed, disputed, or fixed by Chess.com.

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)	C1	Security of processing. A hardcoded, unrotated credential granting read and write access to a live analytics dataset is a failure of confidentiality and integrity controls over that processing.
Art. 32(1)(b)	H1	Same provision, narrower residual risk given the corrected CVSS v4.0 severity, the residual risk is availability-oriented, not confidentiality- or integrity-oriented.
Art. 13(1)(e)	H2	Controllers must name recipients or categories of recipients of personal data at the point of collection. Amplitude was not named.
Art. 8	H2	Processing a child's personal data on the basis of consent requires that consent be given or authorized by the holder of parental responsibility, verified appropriately. No such mechanism was ever described for the Amplitude processing specifically.

Regulatory & Legal Landscape

Chess.com LLC is established in the United States. Chessable Spain S.L. is its designated EEA representative, giving the Austrian DSB and, through cooperation mechanisms, other EU supervisory authorities a route to act. Chessable Ltd is the UK representative, giving the ICO direct jurisdiction over ChessKid's UK child users. The Austrian DSB, German BfDI, and UK ICO were held in BCC across this case's correspondence from the first message. COPPA applies independently in the United States for the platform's US child users, alongside GDPR for its EEA and UK users.

IOC / Reproducible Evidence

```
Package: com.chesskid
Version at disclosure: 3.2.2
res/values/strings.xml:
  amplitude_api_key = 89e2a8ad36ed610a5b68c94e3ccf4412
  amplitude_api_key_dev = (empty)
  google_api_key = AIzaSyDj5RBLsTR_p5mZiJtMUim0tT1LFqyuNBs
  google_crash_reporting_api_key = AIzaSyDj5RBLsTR_p5mZiJtMUim0tT1LFqyuNBs
Extraction: apktool d chesskid.apk && grep -E "amplitude_api_key|google_api_key"
    chesskid/res/values/strings.xml
```

No fresh production build was pulled for this closure report. The findings above are reproducible against the 3.2.2 build reviewed on 24 June 2026; RFI-IRFOS does not claim to know whether the current Google Play build still matches it, and states that gap explicitly instead of assuming continuity.

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-24	R1 sent to press@chess.com and dpo@chess.com. Three findings, three yes/no questions, 90-day embargo set for 2026-09-22.
2026-06-27 through 2026-09-05	Nine further follow-up messages sent across the correspondence, each answered only by an automated press or DPO acknowledgment, never a human reply.
2026-08-21	DPO auto-reply cites reduced capacity from 2026-08-22 through 2026-09-07.
2026-09-05	Eleventh and final outbound message sent, restating the three original questions. Automated acknowledgment received same day. No further correspondence.
2026-09-22	Original 90-day embargo elapses. No human reply had ever been received.
2026-09-23	Case closed and published, one day after embargo, on the terms stated from the first message.

Eleven outbound messages, ten automated acknowledgments, zero human replies, across 91 days. This case has almost no record on the operator’s side at all, there is nothing here to dispute.

Residual Risk & Recommendations

All three findings remain unconfirmed as fixed at the time of publication, because Chess.com never engaged with any of them. RFI-IRFOS recommends, in order of urgency: rotate and remove the hardcoded Amplitude key from the distributed binary and proxy analytics ingestion server-side (C1); apply standard Firebase key restrictions (H1); and name Amplitude explicitly as a processor with a stated lawful basis and a genuine parental consent mechanism, not a general terms-of-service acceptance, for any behavioural analytics running on ChessKid's child user base (H2). Weekly monitoring of the public ChessKid build continues after this publication; any change to any of the three findings will be documented and added to the public record.

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 Severity scored per CVSS v4.0 where a finding was confirmed and reproducible at the time of the original static analysis. RFI-IRFOS reserves the right to weigh real-world blast radius above the bare CVSS score where warranted; one such escalation (H2) applies in this report, documented explicitly in the finding itself. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF RFI-2026-CC-001.