Coordinated Security & Privacy Disclosure, Final Report

UNO! Mobile for Android (package cited inconsistently across correspondence as com.matteljv.uno in R1 and com.mattel.uno in every subsequent message; both are reported here rather than silently reconciled)

Thirteen written notices across seven contact channels, ninety days, one automated auto-reply, zero human replies, and a self-documented Art. 12 access failure

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL SIX FINDINGS UNADDRESSED, SEVEN OF EIGHT CONTACT CHANNELS FAILED OR BOUNCED

Target	Mattel163 Limited, a Mattel/NetEase joint venture
Product audited	UNO! Mobile for Android, package name inconsistent between R1 (com.matteljv.uno) and all subsequent correspondence (com.mattel.uno), a discrepancy disclosed here rather than resolved
Disclosure reference	REF COM.MATTEL.UNO
R1 sent	2026-06-24
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 four hardcoded production credentials, including an AIHelp key granting access to all players' customer-support session data, CVSS v4.0 8.8, unaddressed)

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 performed static analysis of the production UNO! Mobile Android application, a children's card game, and identified three CRITICAL and two HIGH findings: four production credentials hardcoded in plaintext, a platform app secret authenticating the client to Mattel's backend, an AIHelp key granting access to customer-support session data for all UNO! players, and a Facebook client token Meta itself classifies as sensitive and never intended for client-side storage, a voice-chat pipeline built on Agora RTC (Shanghai, subject to China's National Security Law Art. 7 and PIPL) combined with a China-operated AIHelp customer-support integration, with no Art. 44-49 transfer mechanism disclosed for EU children's voice and support data, a pre-consent analytics architecture in which Mattel's own BI ContentProviders initialize ahead of every third-party SDK including Firebase, two boot-time receivers fire without the app ever being opened, and Firebase's own provider is directBootAware, initializing before device unlock, a Network Security Configuration permitting cleartext HTTP to google.com, meaning the pre-consent BI data routed through Google's analytics stack may travel unencrypted on interceptable networks, and Firebase API keys hardcoded with three documented exploitation vectors, security-rule misconfiguration enabling unauthenticated read/write, FCM server-key spoofing enabling fraudulent push at scale, and Remote Config compromise enabling silent behavioral changes that bypass Play Store review.

This case is defined as much by its contact-channel failures as by its technical findings. privacy@mattel.com, the address published in UNO!'s own privacy policy and Play Store listing, is a closed Microsoft 365 distribution group that rejects all external senders, a failure RFI-IRFOS documented as its own Art. 12(1)/13(1)(b) GDPR concern. Across thirteen written notices spanning eight distinct addresses over ninety days, five bounced or failed outright: datenschutz@mattel.de timed out at the server level, net-easelaw@corp.netease.com and mattel@lionheartsquared.eu were invalid, and legal@mattel163.com was likewise a closed group. The only inbound reply across the entire correspondence was a single automated mailbox acknowledgment from dataprivacy@mattel163.com on 9 August, explicitly stating it is an automated response and not engaging with any finding. No human reply was ever received across seven distinct contact channels tried, and none of RFI-IRFOS's four standing questions, on the platform app secret's rotation status, the Art. 44-49 mechanism for children's voice-chat data, Art. 33 notification timing, and why the published privacy contact rejects external mail, ever received an answer.

Scope: Static analysis of the publicly downloaded production UNO! Mobile Android APK, on an authorized test device, only. No Mattel163 account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 24 June 2026 to privacy@mattel.com, bcc the Austrian DSB, German BfDI, and UK ICO. That address, published in UNO!'s own privacy policy and Play Store listing, is configured as a closed Microsoft 365 distribution group that rejects all external senders, a finding RFI-IRFOS documented in its own right. Across thirteen written notices spanning eight distinct addresses over ninety days, five bounced or failed outright, and the only inbound reply across the entire correspondence was a single automated mailbox acknowledgment from dataprivacy@mattel163.com.

ID	Severity	Title
C1	CRITICAL	Four production credentials hardcoded in the public binary
C2	CRITICAL	Voice-chat and support data routed through two China-jurisdiction platforms, no transfer mechanism disclosed
C3	CRITICAL	Pre-consent analytics architecture initializes ahead of every third-party SDK, including before device unlock
H1	HIGH	Firebase API keys hardcoded, three documented exploitation vectors
H2	HIGH	Network Security Config permits cleartext HTTP to google.com

Subject & Operator Analysis

Mattel163 Limited is a joint venture between Mattel, Inc. and NetEase, operating as the actual GDPR data controller for UNO! Mobile through privacy.mattel163.com, distinct from Mattel Inc. itself.

Findings

C1: Four production credentials hardcoded in the public binary

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 8.8

res/values/strings.xml ships four plaintext secrets: mattel_platform_app_secret, which authenticates the client app to Mattel's own backend platform; an AIHelp app key and app ID granting access to customer-support session data for all UNO! players; and a Facebook client token, a value Meta itself classifies as sensitive and specifically advises against storing client-side.

No reply of any kind, across thirteen notices, addressed whether any of these four credentials have been rotated.

Impact: A backend authentication secret and a customer-support-session access key for the entire player base are both extractable from the public APK.

Fix: Rotate all four credentials immediately, and move backend authentication and support-session access off client-side storage entirely.

C2: Voice-chat and support data routed through two China-jurisdiction platforms, no transfer mechanism disclosed

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 binary ships AgoraRtcSDK.dll (113 smali classes) alongside RECORD_AUDIO, BLUETOOTH, and MODIFY_AUDIO_SETTINGS permissions, enabling a full voice-chat pipeline routed through Agora (Shanghai, subject to China's National Security Law Art. 7 and PIPL). The AIHelp customer-support SDK (mattel163.aihelp.net) is likewise China-operated.

No Art. 44-49 GDPR transfer mechanism is disclosed for EU children's voice or support data. No reply of any kind confirmed either a transfer mechanism or an age-verification gate preventing under-16s from voice chat without verified parental consent.

Impact: Children's voice-chat audio and customer-support session data may be routed through PRC-jurisdiction infrastructure with no disclosed transfer mechanism or age-verification gate.

Fix: Disclose the Art. 44-49 transfer mechanism covering Agora and AIHelp, and implement a verified age gate for voice chat.

C3: Pre-consent analytics architecture initializes ahead of every third-party SDK, including before device unlock

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

Mattel's own OmniCommonToolInitProvider (initOrder=1000) and OmniCommonBIInitProvider (initOrder=999) initialize ahead of Vungle, AppLovin, Google Mobile Ads, Firebase, Play Games, BidMachine, SnapKit, and Facebook. Two BOOT_COMPLETED receivers fire without the app ever being opened, and FirebaseInitProvider is directBootAware, initializing before device unlock.

No reply of any kind addressed this finding.

Impact: Behavioral data collection begins before the user has interacted with the app at all, and in some cases before the device is even unlocked, on a children's card game.

Fix: Gate all analytics and BI initialization behind an affirmative consent decision made after the app is actively opened.

H1: Firebase API keys hardcoded, three documented exploitation vectors

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N, 8.8

google_api_key and google_crash_reporting_api_key (both AIzaSyCJTVmeEiv_1en0NU1F6T525BIG3MWxNP8), a second smali-extracted key (AIzaSyB7Mzn6U8hR8pe9PuVYkSqpaVGVhZ5q-1w), and mobilesdk_app_id 1:785285164702:android:59e9c86ff8c0079a are all hardcoded. Three exploitation vectors are documented: Firebase rules misconfiguration enabling unauthenticated read/write, FCM server-key spoofing enabling fraudulent push at scale, and Remote Config compromise enabling silent behavioral changes bypassing Play Store review.

No reply of any kind addressed this finding.

Impact: Three distinct, documented exploitation paths exist against this exposed key set, including one capable of silently changing app behavior without a new Play Store release.

Fix: Rotate all exposed keys, restrict them to the correct package name and signing fingerprint, and confirm deny-by-default Firebase Security Rules.

H2: Network Security Config permits cleartext HTTP to google.com

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.6

res/xml/network_security_config.xml declares cleartextTrafficPermitted="true" for 127.0.0.1 and google.com with subdomains included. Since OmniCommonBIInitProvider routes BI data through Google's analytics stack, pre-consent analytics data may travel unencrypted.

No reply of any kind addressed this finding.

Impact: Pre-consent behavioral analytics data may be transmitted in cleartext and visible on interceptable networks such as public Wi-Fi or corporate proxies.

Fix: Remove the cleartext exception for google.com and enforce HTTPS for all analytics traffic.

Seven Channels, Five Bounces, One Auto-Reply, Zero Humans

privacy@mattel.com, the address published in UNO!'s own privacy policy and Play Store listing, is a closed Microsoft 365 distribution group rejecting all external senders, a finding RFI-IRFOS documented as its own Art. 12(1)/13(1)(b) concern rather than silently working around it. Across thirteen written notices spanning eight distinct addresses over ninety days, datenschutz@mattel.de timed out at the server level, net-easelaw@corp.netease.com and mattel@lionheartsquared.eu were invalid addresses, and legal@mattel163.com was likewise a closed group. The only inbound reply across the entire correspondence was a single automated mailbox acknowledgment from dataprivacy@mattel163.com on 9 August, which explicitly states it is an automated response reviewed only for privacy inquiries and does not engage with any finding. No human reply of any kind was ever received across seven distinct contact channels.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32	Four hardcoded production secrets, including customer-support-session access for all players
C2	GDPR Art. 8, Art. 44, Art. 46; PIPL Art. 13	Undisclosed transfer of children's voice/support data to PRC-jurisdiction platforms
C3	GDPR Art. 5(1)(a), Art. 7, Art. 13; ePrivacy Art. 5(3)	Pre-consent analytics initializing before app open and before device unlock
H1	GDPR Art. 32	Hardcoded Firebase keys with three documented exploitation vectors
H2	GDPR Art. 32	Cleartext-permitted analytics traffic to Google

Disclosure Timeline & Outcome

Date	Event
2026-06-24	R1 sent to privacy@mattel.com, bcc Austrian DSB/German BfDI/UK ICO; a EUR 9,000/18,000/75,000 tiered figure was referenced under the R1 policy then in force – historical record only, not a currently open offer
2026-06-28	privacy@mattel.com confirmed to reject external senders (closed M365 group)
2026-06-30	R2 sent to four new addresses, three bounce immediately; a fourth finding (privacy@mattel.com's Art. 12 access failure) is added
2026-08-09	Follow-up adds four mattel163-domain addresses; automated acknowledgment received from d ataprivacy@mattel163.com, the only inbound reply in the case
2026-08-28	Follow-up, sixty-five days, zero substantive reply
2026-09-12	Follow-up, eighty days since disclosure, most recent message on file
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Fix privacy@mattel.com so it can receive external GDPR correspondence, resolving the self-documented Art. 12(1) access failure.
- Rotate all four hardcoded credentials and both Firebase keys, and move backend/suppor t-session authentication off the client.
- Disclose the Art. 44-49 transfer mechanism covering Agora and AIHelp, and implement a verified age gate for voice chat.
- Gate all analytics/BI initialization behind an affirmative consent decision made after active app use.
- Remove the cleartext exception for google.com in the Network Security Configuration.

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. GDPR Art. 5, 7, 8, 12, 13, 32, 33, 44, 46. REF COM.MATTEL.UNO.