# Coordinated Privacy Disclosure, Final Report

## Roblox Android (com.roblox.client)

Roblox Corporation (NYSE: RBLX), San Mateo, California, USA

**AUTOMATED ACKNOWLEDGMENT ONLY · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ONE DAY AFTER THE EMBARGO, TEN MESSAGES, TEN IDENTICAL BOT REPLIES, ZERO HUMAN REPLY**

| | |
|---|---|
| **Target** | Roblox, a global gaming and creation platform whose user base is majority under 13 |
| **Package** | com.roblox.client |
| **Operator** | Roblox Corporation (NYSE: RBLX), San Mateo, California, USA |
| **Initial Disclosure** | 2026-06-19, first contact; full technical findings sent 2026-06-27 |
| **Original Embargo** | 2026-09-24 (90 days from disclosure, as stated in the original notice) |
| **Report Published** | 2026-09-25, one day after the embargo, an internal publishing gap, not a change in terms |
| **Regulators** | Austrian DSB, CERT.at |
| **Total Outbound Messages** | 10, sent on a sustained weekly cadence to security@roblox.com, cc'ing privacy@roblox.com and press@roblox.com. |
| **Inbound Replies** | 10, every one of them an identical automated acknowledgment from dart+noreply@roblox.com ("report security bugs via HackerOne") and/or press+noreply@roblox.com. No substantive human reply was ever received. |

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

## Contents

**1 Executive Summary** **4**

**2 Subject & Operator Analysis** **6**

**3 Ten Messages, Ten Bot Replies, Zero Human Reply** **6**

**4 Findings** **6**

4.1 RB01: Full Contact Book Uploaded: Names and Phone Numbers of Non-Users, No Visible Under-13 Gate . . . . . 7

4.2 RB02: Behavioral Ad Profiling via the Android Topics API, No Visible Under-13 Gate . . . . . 8

4.3 RB03: Child-Status Flag Passed via JNI Into the Game Engine, Potentially Reachable by Millions of Third-Party Creators . . . . . 9

4.4 RB06: Dormant Tencent/QQ China Endpoints Hardcoded in the Global Production Build . . . . . 10

4.5 RB04: Screen-Capture Callback Registered With No Disclosed Use Case . . . 10

4.6 RB05: Exported SMS-Retriever Receiver With No Permission Restriction . . . . 11

**5 Data Protection, Article by Article** **11**

## Executive Summary

Beginning 19 June 2026, RFI-IRFOS disclosed to Roblox Corporation that its Android app queries ContactsContract.Data.CONTENT_URI for both phone number and display name mimetypes simultaneously, packaging the result under a getContacts protocol name for transmission to Roblox's servers. The people whose data is uploaded this way, parents, siblings, classmates, are not Roblox users and have not consented to anything. Roblox's own age-verification flag, under13, exists in the codebase, but no conditional check gating this specific contact-upload call on that flag is visible in static analysis.

Two further findings share the same underlying gap. The Android Privacy Sandbox Topics API, which infers a user's interest categories from app usage for behavioral ad targeting, is actively called with no visible under13 gate in the reviewed binary. Separately, the under13 flag itself is embedded in StartGameParams and passed via JNI into the native Lua game engine, meaning it may be queryable by any of Roblox's millions of independent game creators, a potential channel for child-status data to reach parties entirely outside Roblox's own platform controls. Both findings are held at HIGH under an explicit RFI-IRFOS blast-radius escalation: Roblox's user base is majority under 13, a legally protected population under COPPA and GDPR Art. 8, and any gap in age-gating at this platform's scale carries materially higher real-world stakes than the same technical gap on a general-audience app.

Ten messages were sent to security@roblox.com on a sustained weekly cadence across 76 days, cc'ing privacy@roblox.com and press@roblox.com and, on later rounds, the Austrian DSB and CERT.at. Every single reply received, ten in total, was an identical automated acknowledgment, either from dart+noreply@roblox.com redirecting all reports to a HackerOne bug-bounty program, or from press+noreply@roblox.com confirming only that a media inquiry had been logged. Not one substantive, human-authored reply was ever received. The 90-day embargo, set at first contact, elapsed on 24 September 2026. This report and the accompanying closure notice publish one day 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 Roblox Android application (com.roblox.client, version 2.725.1142, 97 MB, SHA-256 4bae738b932e7e500f6af69c6d443b76f335222aa6af6866a440776bd26b8632), as pulled and reviewed on 20 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Roblox's backend infrastructure was performed.

**Disposition**

Six findings were disclosed on 19-27 June 2026, re-scored under CVSS v4.0. A full-contact-book upload, extracting names and phone numbers of non-users from a child's device with no visible age gate, reaches HIGH on the computed CVSS score alone. Two further findings, behavioral ad profiling via the Android Topics API with no visible under-13 gate, and a child-status flag (isUnder13) passed via JNI into the game engine where it is potentially reachable by millions of third-party game creators, are held at HIGH under an explicit blast-radius escalation given Roblox's confirmed majority-under-13 user base. A hardcoded set of dormant Tencent/QQ endpoints in the global build corrects to MEDIUM. An exported SMS-retriever receiver and a screen-capture callback both correct to LOW. Ten messages were sent on a sustained weekly cadence; every single reply received was an identical automated acknowledgment redirecting to a bug-bounty program, and not one substantive human reply was ever received.

| ID | Severity | Title |
|---|---|---|
| RB01 | HIGH | Full Contact Book Uploaded: Names and Phone Numbers of Non-Users, No Visible Under-13 Gate |
| RB02 | HIGH | Behavioral Ad Profiling via the Android Topics API, No Visible Under-13 Gate |
| RB03 | HIGH | Child-Status Flag Passed via JNI Into the Game Engine, Potentially Reachable by Millions of Third-Party Creators |
| RB06 | MEDIUM | Dormant Tencent/QQ China Endpoints Hardcoded in the Global Production Build |
| RB04 | LOW | Screen-Capture Callback Registered With No Disclosed Use Case |
| RB05 | LOW | Exported SMS-Retriever Receiver With No Permission Restriction |

## Subject & Operator Analysis

Roblox is a global gaming and creation platform operated by Roblox Corporation (NYSE: RBLX), whose own reporting confirms a majority-under-13 user base, a directly relevant fact for every finding in this report.

Several genuine positives are worth naming. allowBackup is correctly set to false. largeHeap is correctly set to false. resizeableActivity is correctly set to false, a consistent security posture. Primary deep links (games, catalog) are correctly restricted to the HTTPS scheme. An age-verification flag (under13) does exist in the codebase, confirming Roblox does attempt to track child status internally, the finding here is about where that flag's protections do and do not reach, not that the flag is absent.

## Ten Messages, Ten Bot Replies, Zero Human Reply

This case's correspondence record involved a working contact channel from the first message; no address bounced. Ten messages were sent to security@roblox.com on a sustained weekly cadence, cc'ing privacy@roblox.com and press@roblox.com and, on later rounds, the Austrian DSB and CERT.at. Every single reply received, ten in total, was an identical automated acknowledgment: dart+noreply@roblox.com redirecting all reports to Roblox's HackerOne bug-bounty program regardless of content, and/or press+noreply@roblox.com confirming only that a media inquiry had been logged. Not one substantive, human-authored reply addressing any specific finding was ever received.

## Findings

### RB01: Full Contact Book Uploaded: Names and Phone Numbers of Non-Users, No Visible Under-13 Gate

**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. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.**

The app queries ContactsContract.Data.CONTENT_URI with a combined filter for both phone_v2 and name mimetypes, extracting the full phone book and packaging it under a getContacts protocol name for transmission to Roblox's servers. The people whose data is uploaded, parents, siblings, classmates, are not Roblox users and have not consented. Roblox's own under13 flag exists in the codebase, but no conditional check gating this specific contact-upload call on that flag is visible in static analysis.

```
const-string v12, "vnd.android.cursor.item/phone_v2"
const-string v13, "vnd.android.cursor.item/name"
const-string v5, "mimetype IN (?, ?)"
sget-object v3, Landroid/provider/ContactsContract$Data;->CONTENT_URI:Landroid/net/Uri
    ;
const-string v3, "phonenumber" ; field extracted to JSON
const-string v4, "getContacts" ; protocol name
```

**Impact:** Third-party personal data, names and phone numbers of people who are not Roblox users and never consented, is uploaded from a device population that is majority minors, with no visible age-based gate on this specific call.

**Fix:** Remove full-phone-book upload entirely, or gate it behind explicit, verifiable parental consent with no default-on behavior; implement friend-finding via username search instead. No confirmation that this has occurred was ever received.

### RB02: Behavioral Ad Profiling via the Android Topics API, No Visible Under-13 Gate

**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 app actively calls TopicsManager.get() and issues a GetTopicsRequest, the Android Privacy Sandbox mechanism that infers interest categories from app usage history for behavioral ad targeting. All three AdServices permissions (ACCESS_ADSERVICES_TOPICS, ACCESS_ADSERVICES_AD_ID, ACCESS_ADSERVICES_ATTRIBUTION) are declared and used. No conditional check gating this call on under13 == false is visible in static analysis.

```
invoke-static {p1}, Landroid/adservices/topics/TopicsManager;->get(Landroid/content/
    Context;)Landroid/adservices/topics/TopicsManager;
invoke-static {}, Lm4/c;->a()Landroid/adservices/topics/GetTopicsRequest$Builder;
invoke-virtual {v0, v1}, Landroid/adservices/topics/GetTopicsRequest$Builder;->
    setAdsSdkName(Ljava/lang/String;)
```

**Impact:** If this call fires for accounts already flagged under13 in Roblox's own data, behavioral ad profiling of children under 13 occurs, a direct COPPA violation and a GDPR Art. 8 gap, at the scale of Roblox's entire under-13 user population. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because Roblox's confirmed majority-under-13 user base is a legally protected population under COPPA and GDPR Art. 8, and a gap in age-gating behavioral ad profiling at this platform's scale carries materially higher real-world stakes than the same technical gap elsewhere.

**Fix:** Wrap all AdServices API calls in an explicit if (!isUnder13) guard, audit third-party SDKs for independent Topics API calls, and remove all three AdServices permissions for under-13 account sessions. No confirmation that this has occurred was ever received.

### RB03: Child-Status Flag Passed via JNI Into the Game Engine, Potentially Reachable by Millions of Third-Party Creators

**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.**

StartGameParams, the parameter bundle passed from the Android app layer to the native Lua game engine via JNI, includes an isUnder13 boolean field. If this field is reachable through the Roblox Studio Lua scripting API available to game creators, any of Roblox's 8 million-plus independent creators could query whether a specific player is under 13, sensitive child-protection data that should remain under Roblox's own platform control, not delegated outward.

```
.field private final isUnder13:Z
iput-boolean p11, p0, Lcom/roblox/engine/jni/autovalue/AutoValue_StartGameParams;->
    isUnder13:Z
invoke-virtual {p0}, Lcom/roblox/engine/jni/autovalue/StartGameParams;->isUnder13()Z
```

**Impact:** If exposed through the Lua scripting API, any of millions of independent game creators could target monetization mechanics specifically at players known to be under 13, a child-safety exposure at platform scale. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because exposure of a child-safety flag to Roblox's population of 8 million-plus independent game creators is a distinct, platform-scale child-protection concern, not a narrow technical gap.

**Fix:** Verify whether isUnder13 is accessible through the Roblox Studio Lua API; if it is, remove that exposure and enforce child-protection restrictions exclusively at the platform layer. No confirmation that this has occurred was ever received.

### RB06: Dormant Tencent/QQ China Endpoints Hardcoded in the Global Production Build

**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.**

roblox.qq.com and luobu.qq.com, Tencent-operated servers associated with Roblox's former China partnership, remain hardcoded in the global APK reviewed (version 2.725.1142, June 2026), years after that partnership's operational window. Whether the referencing code paths are reachable for non-China users could not be confirmed from static analysis alone.

```
https://roblox.qq.com/?webview=true0409
https://luobu.qq.com/fx/a20210622fxy/index.html
https://roblox.qq.com/m/m202106/newsDetail.html?newsid=14640697
```

**Impact:** If any referencing code path remains reachable for non-China users, data could route through Tencent-operated infrastructure without disclosure; even as unreachable dead code, hardcoded partner endpoints in a global build are a compliance-hygiene signal worth resolving.

**Fix:** Strip all roblox.qq.com/luobu.qq.com references from the global release build and use separate build flavors for China-specific distribution. No confirmation that this has occurred was ever received.

### RB04: Screen-Capture Callback Registered With No Disclosed Use Case

**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.**

The app registers an Activity ScreenCaptureCallback, notified in real time whenever a user screenshots the app in the foreground, using the DETECT_SCREEN_CAPTURE permission, with no disclosed use case located in the app's privacy documentation.

```
invoke-virtual {p1, v1, v0}, Landroid/app/Activity;->registerScreenCaptureCallback(
    Ljava/util/concurrent/Executor;Landroid/app/Activity$ScreenCaptureCallback;)V
```

**Impact:** Screenshot activity is monitored in real time on a platform whose user base is majority minors, with no disclosed purpose; the practical exploitation path requires local conditions the static review could not establish, which keeps the computed score low despite the lack of disclosure.

**Fix:** Disclose the use case explicitly, limit detection to specific gameplay or DRM-relevant screens, or remove the permission. No confirmation that this has occurred was ever received.

### RB05: Exported SMS-Retriever Receiver With No Permission Restriction

**LOW, CVSS v4.0 AV:P/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 1.0.**

SMSBroadcastReceiver is exported with no permission restriction and listens for the Google SMS Retriever broadcast used to auto-read six-digit OTP codes. The outer Google SMS Retriever hash check limits forgery, but the exported declaration itself is unnecessarily permissive, allowing any app on the device to send a spoofed SMS_RETRIEVED broadcast.

```
com.roblox.client.sms.SMSBroadcastReceiver (android:exported="true")
const-string p1, "com.google.android.gms.auth.api.phone.SMS_RETRIEVED"
```

**Impact:** Any other app on the same device could send a spoofed SMS_RETRIEVED broadcast toward this receiver; the Google-side hash check materially limits practical forgery, which keeps the computed score low.

**Fix:** Add android:permission="com.google.android.gms.auth.api.phone.permission.SEND" to the receiver declaration. No confirmation that this has occurred was ever received.

## Data Protection, Article by Article

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

| Article/Rule | Finding | Basis |
|---|---|---|
| GDPR Art. 6, Art. 8; COPPA | RB01 | Third-party contact data uploaded from a device population that is majority minors, no visible age gate. |
| GDPR Art. 8; ePrivacy Directive; COPPA | RB02 | Behavioral ad profiling via the Topics API with no visible under-13 gate. |
| GDPR Art. 25; child-protection principle | RB03 | Child-status flag potentially reachable by millions of third-party creators. |
| Art. 44 (contingent), Art. 5(1)(f) | RB06 | Dormant third-country partner endpoints hard-coded in the global build. |

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, RB01 reaches HIGH on its computed CVSS v4.0 score alone, no editorial escalation applied; RB02 and RB03 are held at HIGH under an explicit RFI-IRFOS blast-radius escalation given Roblox's confirmed majority-under-13 user base, a legally protected population under COPPA and GDPR Art. 8; RB06 corrects to MEDIUM on its own computed band; RB04 and RB05 correct to LOW on their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: ROBLOX-2026-R1.