



Coordinated Security & Privacy Disclosure, Final Report

BIGO LIVE (sg.bigo.live)

BIGO Technology Pte. Ltd. (Singapore), part of the YY Inc. group. Livestreaming application for Android.

**PUBLISHED 22 OCTOBER 2026, 90 DAYS AFTER DISCLOSURE · PARTIAL SILENT
REMEDATION · TWO OF FOUR FINDINGS STILL OPEN IN BUILD 6.55.2**

Target	BIGO LIVE, a livestreaming and social video application for Android
Package	sg.bigo.live. Disclosure analysis of 24 July 2026 (build and hash not archived). Re-check of 22 October 2026: version 6.55.2, versionCode 4168, targetSdk 36.
Operator	BIGO Technology Pte. Ltd. (Singapore). Legal contact legal@bigo.tv, external counsel in copy from 23 September 2026.
Initial Disclosure	2026-07-24 (sent 2026-07-23 23:47 UTC)
Embargo	2026-10-22 (90 days from delivery of the first notice)
Publication	2026-10-22, independent of any reply
Regulators in CC	Austrian DSB, CERT.at, German BfDI (first notice and follow-ups until 24 August 2026)
Inbound Messages	3 from BIGO legal: 5 August, 23 September and 21 October 2026. No answer to the three questions at any point.
Build re-checked	6.55.2, pulled from Google Play on 22 October 2026. SHA-256 of base.apk: e68b03a2da2054e3fc251f971cece6767d6df17741e09e6660f2e10ace566bce

security@rfi-irfos.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	5
3	Architecture & Data Flow	5
4	Findings	6
4.1	C1: Hardcoded Plain-HTTP Address on the China Telecom ChinaNet Backbone (AS4134, Shenzhen)	6
4.2	H1: READ_CALL_LOG, ANSWER_PHONE_CALLS and CALL_PHONE in a Livestreaming Application	7
4.3	M1: Production Firebase API Key Hardcoded in String Resources	8
4.4	L1: Cleartext Traffic Permitted in the Base Network Security Configuration . . .	8
5	Impact Analysis	9
6	The Complete Chain	9
7	Data Protection, Article by Article	9
8	Regulatory & Legal Landscape	10
9	IOC / Reproducible Evidence	10
10	Disclosure Timeline & Outcome	11
11	Residual Risk & Recommendations	12

Executive Summary

On 24 July 2026 RFI-IRFOS notified BIGO that BIGO LIVE contained a hardcoded plain-HTTP address on the China Telecom ChinaNet backbone (AS4134, Shenzhen), <http://121.11.65.96:9090/adlist>, in an application that also requests access to the call log, the ability to place and answer calls and the ability to disable the lock screen. The notice asked three written questions: the legal basis and purpose of the call permissions, the transfer mechanism for the backbone connection, and whether the Data Protection Officer and a data protection impact assessment were in place.

Over 90 days BIGO legal responded three times. The first reply offered a call. The second, on 23 September, cited a fee schedule, referred to its own vulnerability program and stated that the ChinaNet code had been purged, without a record of when the address was reachable. The third, on 21 October, attached an earlier RFI-IRFOS message of 27 June that lists public disclosure as free, with or without a response. None of the three answered a question. RFI-IRFOS retracted its own earlier statement that no fee figure existed in the correspondence, because the 27 June message contains an options table. Publication was never linked to a payment in any message.

A re-check of the current Google Play build, 6.55.2, shows partial remediation without any announcement: the hardcoded address, the cleartext base configuration and `DISABLE_KEYGUARD` are gone. `READ_CALL_LOG`, `ANSWER_PHONE_CALLS` and `CALL_PHONE` remain declared and referenced in code, and the production Firebase key is unchanged. This report publishes the record on the date announced from the first message.

Scope: Deep Scan of the public Google Play build of BIGO LIVE (sg.bigo.live). The original analysis of 24 July 2026 is documented in the first notice. The re-check of 22 October 2026 covers build 6.55.2 pulled from a device with adb, decompiled with apktool, with manifest, network security config, string resources and smali inspected. No traffic was captured, no account was created, no live API was called with the Firebase key. A declared permission and a code reference show capability, they do not show data flow.

Disposition

On 24 July 2026 RFI-IRFOS disclosed to BIGO that the Android application BIGO LIVE shipped a hardcoded connection to a server on the China Telecom ChinaNet backbone, a cleartext network configuration, four call and lock-screen permissions and a production Firebase key. BIGO answered on 23 September that the ChinaNet reference was a legacy test artifact, that the code had been purged and that `READ_CALL_LOG` would be deprecated. A re-check of build 6.55.2 on 22 October 2026 confirms the removal of the hardcoded address, the cleartext base configuration and `DISABLE_KEYGUARD`. `READ_CALL_LOG`, `ANSWER_PHONE_CALLS`, `CALL_PHONE` and the Firebase key remain.

ID	Severity	Title
C1	CRITICAL	Hardcoded Plain-HTTP Address on the China Telecom ChinaNet Backbone (AS4134, Shenzhen)
H1	MEDIUM	READ_CALL_LOG, ANSWER_PHONE_CALLS and CALL_PHONE in a Livestreaming Application
M1	MEDIUM	Production Firebase API Key Hardcoded in String Resources
L1	LOW	Cleartext Traffic Permitted in the Base Network Security Configuration

Subject & Operator Analysis

BIGO LIVE is a livestreaming application operated by BIGO Technology Pte. Ltd., Singapore, part of the YY Inc. group. BIGO operates a Security Response Center at security.bigo.sg and named external counsel as the channel for legal correspondence from 23 September 2026.

RFI-IRFOS approached BIGO under the same rules that apply to every application in its campaign of more than 300 applications: a first notice, a fixed 90-day period, publication on the announced date, and no link between publication and any commercial offer.

Architecture & Data Flow

The findings sit in three layers of the Android package. The network layer holds the hard-coded address and the network security configuration. The permission layer holds the call-related permissions in the manifest and their references in code. The credential layer holds the Firebase key in string resources. The package also bundles large third-party SDK sets from Facebook, Tencent and Alibaba.

RFI-IRFOS captured no traffic. The architecture description is limited to what the shipped package contains.

Findings

C1: Hardcoded Plain-HTTP Address on the China Telecom ChinaNet Backbone (AS4134, Shenzhen)

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.3. Editorial severity CRITICAL, see escalation below. Status in build 6.55.2: removed.

The analysis of 24 July 2026 found the address `http://121.11.65.96:9090/adlist` hardcoded in the shipped application. 121.11.65.96 belongs to the ChinaNet backbone of China Telecom in Shenzhen, a state-owned carrier. The request uses plain HTTP, so any party on the path can read and alter it. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.3 to CRITICAL because the destination is operated by a carrier that is subject to Article 7 of China's National Intelligence Law, because it sits in a livestreaming application that also declares call-log and call-control permissions, and because BIGO has not stated a legal basis or transfer mechanism for it. BIGO states the reference was a legacy testing artifact that was never active in production and that the code has been purged. Build 6.55.2 contains no occurrence of the address in smali, resources, native libraries or assets.

```
analysis 2026-07-24 (first notice):  
http://121.11.65.96:9090/adlist
```

```
re-check 2026-10-22, build 6.55.2 (versionCode 4168):  
grep -rIl -E "121\.11\.65\.96|:9090/adlist" apktool_out -> no match  
grep -rIaE "121\.11\.65\.96" lib assets unknown original -> no match
```

The removal confirms that the address existed in a shipped build. BIGO's statement that it was never active cannot be checked from outside, and BIGO provided no build number, date range or log. The question of which transfer mechanism applied for the period the address was present in shipped builds remains unanswered.

Bundled in the same build at the time of the first notice were 911 Facebook classes, 30 Tencent MMKV and Xlog classes and 7 Alibaba classes. Build 6.55.2 contains 964 Facebook, 31 Tencent (15 of them MMKV or Xlog) and 7 Alibaba smali files. The counting method of 24 July is not archived, so these numbers are not compared with each other.

Impact: A plain-HTTP request to a fixed address on a state-owned carrier network from every installation that reached the code path, readable and modifiable by any party on the network path, in an application whose own legal team has not stated a legal basis for it.

Fix: Publish the build range in which the address was present and the traffic that used it, state the Article 44 to 46 GDPR transfer mechanism for that period, and keep the hardcoded endpoint out of future builds.

H1: READ_CALL_LOG, ANSWER_PHONE_CALLS and CALL_PHONE in a Livestreaming Application

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.7. Status in build 6.55.2: open.

Build 6.55.2 declares READ_CALL_LOG, ANSWER_PHONE_CALLS and CALL_PHONE and references the corresponding Android APIs in code. All three are runtime permissions that the user must grant, which is why the vector uses active user interaction. READ_CALL_LOG gives access to the call history, ANSWER_PHONE_CALLS and CALL_PHONE allow the application to answer and end calls and to place calls. DISABLE_KEYGUARD, disclosed in July, is no longer declared. BIGO states that READ_CALL_LOG was implemented for user-authorized login verification and that the functionality will be deprecated in upcoming releases. The permission is still declared in 6.55.2.

```
aapt2 dump permissions base.apk (6.55.2):
uses-permission: name='android.permission.ANSWER_PHONE_CALLS'
uses-permission: name='android.permission.READ_CALL_LOG'
uses-permission: name='android.permission.CALL_PHONE'
(DISABLE_KEYGUARD: not declared)

smali_classes4/sg/bigo/live/r94.smali:15
    Landroid/provider/CallLog$Calls; ->CONTENT_URI
smali_classes5/sg/bigo/live/rpb.smali:147
    Landroid/telecom/TelecomManager; ->endCall()Z
smali_classes6/sg/bigo/live/dwp.smali
    TelecomManager acceptRingingCall reference
```

On a device that has not granted the permissions, the system reports granted=false for all three. This report makes no statement about call data leaving a device. The record shows that the application requests and uses call-related APIs without any stated purpose for ANSWER_PHONE_CALLS and CALL_PHONE, and that BIGO has named a purpose for READ_CALL_LOG only.

Impact: Capability to read the call history and to answer, end and place calls on devices where the user grants the permissions, with a stated purpose for one of three permissions.

Fix: State the purpose and the Article 6 or 7 GDPR legal basis for each of the three permissions, remove the ones without a documented purpose, and request them only at the moment of use.

M1: Production Firebase API Key Hardcoded in String Resources

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N, 6.3. Status in build 6.55.2: open.

The key `AIzaSyBrWcUkgUhXg-q0Eh9ZG2v6Y6QFGNCIGpA` is stored in `res/values/strings.xml` as `google_api_key` and as `google_crash_reporting_api_key` in build 6.55.2, identical to the key named in the first notice. RFI-IRFOS did not call any live API with this key, that step belongs to a later stage of a disclosure. The vector assumes that the exposure of a Google API key creates quota and billing exposure and limited data exposure depending on the restrictions BIGO has configured, and that an attacker needs those restrictions to be absent, which is why attack requirements are marked present.

`res/values/strings.xml (6.55.2):`

```
<string name="google_api_key">AIzaSyBrWcUkgUhXg-q0Eh9ZG2v6Y6QFGNCIGpA</string>
<string name="google_crash_reporting_api_key">AIzaSyBrWcUkgUhXg-q0Eh9ZG2v6Y6QFGNCIGpA
  </string>
```

Impact: A credential-type string in every installation. Its actual reach depends on the API restrictions and the Firebase security rules of BIGO's project.

Fix: Restrict the key by package name and signing certificate and to the APIs the application needs, review the Firebase security rules, and rotate the key if restrictions were absent.

L1: Cleartext Traffic Permitted in the Base Network Security Configuration

LOW, CVSS v4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 2.3. Status in build 6.55.2: remediated.

The first notice reported `cleartextTrafficPermitted=true` in the base configuration. Build 6.55.2 sets `cleartextTrafficPermitted=false` in the base configuration and permits clear-text only for localhost.

`res/xml/r.xml (6.55.2):`

```
<base-config cleartextTrafficPermitted="false">
<domain-config cleartextTrafficPermitted="true">
  <domain includeSubdomains="true">localhost</domain>
```

Impact: Historic exposure of all application traffic to downgrade on hostile networks, closed in the current build.

Fix: None required. Keep the base configuration at false.

Impact Analysis

Users of BIGO LIVE are people who stream and watch video and who connect their phone number and contacts to a social product. For them, the relevant points are call-history access, call control and a network request to a carrier network under a foreign intelligence law. The record shows capability and presence in shipped code. It shows no proven transfer of personal data.

The Complete Chain

Point of contact: a user installs BIGO LIVE from Google Play. Capability: the package requests call-history and call-control permissions in the manifest and carries a hardcoded plain-HTTP address on the ChinaNet backbone (until a build before 6.55.2). Exposure: the address was readable and alterable on the network path, the call permissions depend on the user's grant, the Firebase key depends on BIGO's restrictions. Accountability: three questions were put to BIGO for 90 days, covering purpose and legal basis of the call permissions, the transfer mechanism for the backbone address and the involvement of the Data Protection Officer in a DPIA. None was answered. The address, the cleartext base configuration and DISABLE_KEYGUARD were removed without notice during this period.

The silent removal is the strongest indicator in the record that the first notice described real code. BIGO's own statement of 23 September uses the word purged for the ChinaNet code.

Data Protection, Article by Article

Article	Question raised by the record
Art. 5(1)(c)	Data minimisation: why does a livestreaming application declare READ_CALL_LOG, ANSWER_PHONE_CALLS and CALL_PHONE?
Art. 5(2)	Accountability: BIGO has not shown the purpose per permission.
Art. 6 and 7	Legal basis and consent for call-history access: BIGO names login verification for READ_CALL_LOG only.
Art. 25	Data protection by design: call permissions still declared in 6.55.2 after the announced deprecation.
Art. 35	Impact assessment: no DPIA statement for the permissions or the backbone connection.
Art. 44 to 46	Transfer mechanism: none stated for the period in which the ChinaNet address was in shipped builds.

These are questions that arise from the technical record. They are not findings of a violation. Legal assessment lies with the supervisory authorities.

Regulatory & Legal Landscape

The Austrian Data Protection Authority, CERT.at and the German BfDI received the first notice and the follow-ups of 5 August, 15 August and 24 August 2026 in copy.

Disclosure follows ISO/IEC 29147. The analysis of a publicly downloadable application build is protected research under Article 17 of the Austrian Staatsgrundgesetz and the Forschungsfreiheitsgesetz. China's National Intelligence Law, Article 7, is cited as published law about the obligations of Chinese organisations and citizens to support national intelligence work. Its application to a specific carrier and a specific request is not established by this report.

IOC / Reproducible Evidence

Item	Value
Package	sg.bigo.live
Re-check build	6.55.2, versionCode 4168, targetSdk 36, pulled 2026-10-22
base.apk SHA-256	e68b03a2da2054e3fc251f971cece6767d6df17741e09e6660f2e10ace566bce
split_config.arm64_v8a.apk SHA-256	35555e056d5c1c240e0fc3c0d8d23d6ad8de9d4342d3c3148751b731c9888a81
split_config.de.apk SHA-256	925b0b6355dc046cc078ea33002b564baa862d2d0bf1236930002a8ee529de43
split_config.xxhdpi.apk SHA-256	1aa13fc3eaa8ca10e19613a483b139085bc423f7ad33972e1ee949c80ebd8bb8
Disclosed address (24 July 2026)	http://121.11.65.96:9090/adlist, AS4134 China Telecom, Shenzhen
Firebase key	AlzaSyBrWcUkgUhxg-q0Eh9ZG2v6Y6QFGNCIGpA
Reproduction	Install the Google Play build, aapt2 dump permissions base.apk, apktool d base.apk, then inspect res/xml/r.xml, res/values/strings.xml and the smali references listed under H1.

The package of 24 July 2026 was not archived. The comparison with that state rests on the first notice, which names each item.

Disclosure Timeline & Outcome

Date	Event
2026-06-27	Earlier RFI-IRFOS message to BIGO, cited by BIGO on 21 October. Its options table lists Public Disclosure as free, with or without a response.
2026-07-23 / 07-24	First notice to feedback@bigo.tv with DSB, CERT.at and BfDI in copy. Three questions and a 90-day embargo.
2026-08-05	BIGO legal acknowledges an internal review and offers a call. RFI-IRFOS asks for written answers and restates the questions.
2026-08-15	Follow-up. Embargo unchanged.
2026-08-24	Follow-up. Embargo unchanged.
2026-09-12	Follow-up with deadline 19 September. No answer.
2026-09-23	BIGO legal replies: refers to its Security Response Center, cites a fee schedule, states the ChinaNet code was a testing artifact and has been purged, names login verification for READ_CALL_LOG. RFI-IRFOS answers the same day sentence by sentence.
2026-10-17	Notice: 5 days to publication.
2026-10-21	BIGO legal replies with the 27 June message attached and announces no further responses. RFI-IRFOS corrects its earlier statement about the fee table and restates the three questions.
2026-10-22	Publication.

Outcome: three inbound messages, none answering a question. Publication was announced as unconditional in every message from the first notice and did not depend on any reply.

Residual Risk & Recommendations

Open in build 6.55.2: three call-related permissions without a stated purpose for two of them, and the unchanged Firebase key with unknown restrictions. Closed without announcement: the hardcoded ChinaNet address, the cleartext base configuration and DISABLE_KEYGUARD.

RFI-IRFOS pulls the BIGO LIVE package weekly and compares permissions, SDKs and endpoints against its archive. Any change is added to the public record without resetting the embargo. A silent fix of a reported item is documented as such.

Recommendations for BIGO: answer the three questions in writing, publish the build range and purpose of the removed backbone address, document the purpose or remove ANSWER_PHONE_CALLS, CALL_PHONE and READ_CALL_LOG, and review the restrictions of the Firebase key.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria Severity scored per CVSS v4.0 (CVSS-B) with the

FIRST reference calculator logic. One escalation applies in this report (C1), documented explicitly in the finding. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF BIGO-2026-R1.