Coordinated Privacy Disclosure, Final Report

trivago Android (com.trivago)

trivago N.V., Kesselstraße 5-7, 40221 Düsseldorf, Germany

REPEATED VULNERABILITY-DISCLOSURE-PROGRAM REDIRECT, SELF-DECLARED CLOSED, THEN SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ON THE ORIGINAL EMBARGO DATE

Target	trivago, a hotel and travel price-comparison Android app
Package	com.trivago
Operator	trivago N.V., Düsseldorf, Germany
Initial Disclosure	2026-06-27
Original Embargo	2026-09-25 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, on the original embargo date
Regulators	Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW, lead SA), Austrian DSB
Total Outbound Messages	5, across 71 days, to MOD_Security@trivago.com and privacy@trivago.com.
Inbound Replies	4, on 27 June, 1 July, 10 July, and 13 July 2026, all form replies from trivago's Zendesk support desk repeating that reports should be filed through trivago's Vulnerability Disclosure Program on YesWeHack, without addressing any specific technical finding. The 13 July reply explicitly stated trivago considered the matter closed on its end; no reply of any kind followed a 48-hour, finding-by-finding response deadline set on 10 July, and none has been received since.

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

Contents

Executive Summary

On 27 June 2026, RFI-IRFOS disclosed to trivago N.V. that its Android app ships a native library, libakamaibmp.so, compiled for four architectures and run in an isolated process (:com.akamai.webview.process), branded in the manifest as an Akamai component. Independent analysis found three separate layers obscuring its true origin: runtime string decryption via a compiled method, a native binary that resists static analysis, and a dedicated, separately named process. The library initializes at initOrder=100, before any consent mechanism can run. Firebase Remote Config, with 57 compiled classes, allows trivago to reconfigure tracking behavior after installation without an app-store update, and cleartextTrafficPermitted is set to true as the app's base configuration, meaning hotel search queries can transit unencrypted HTTP.

A second finding names a production-shipped developer tool, not a single tracking flow: ChuckerInterceptor is compiled into the production binary alongside a RetentionManager configured for indefinite (FOREVER) log retention, a debug network logger that should never reach a version users download, retaining a full record of network activity on-device indefinitely. Separately, a Facebook cross-app signal receiver (PPML/IReceiverService) allows Meta to receive signals without user interaction, and all four Android Privacy Sandbox APIs are declared simultaneously, alongside a dedicated AppsFlyer Privacy Sandbox endpoint.

Five messages were sent across 71 days, to MOD_Security@trivago.com and privacy@trivago.com, cc'ing the German LDI NRW and the Austrian DSB. Four replies were received, on 27 June, 1 July, 10 July, and 13 July 2026, every one a Zendesk-generated form reply from trivago's User Support desk, redirecting to trivago's Vulnerability Disclosure Program on the third-party platform YesWeHack, without engaging any specific technical finding. On 10 July 2026, RFI-IRFOS set a 48-hour deadline for a named, dated, finding-by-finding response; trivago's 13 July reply, one day past that deadline, repeated the same VDP redirect and stated plainly that trivago considered the matter closed on its end. No reply of any kind followed two further messages, on 5 August and 6 September 2026. The 90-day embargo, set at first contact, elapses today, 25 September 2026, and this report publishes on that date.

Scope: Root-level static analysis of the production trivago Android application (com.trivago, version 6.63.0), as reviewed on 27 June 2026. No dynamic instrumentation, live traffic capture, or interaction with trivago's, Akamai's, or Meta's backend infrastructure was performed.

Disposition

Six findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. Cleartext traffic permitted by default and a production-shipped debug HTTP interceptor configured for indefinite log retention both reach HIGH on the computed CVSS score alone. An obfuscated native SDK disguised as an unrelated vendor's product, post-install remote tracking reconfiguration, an undisclosed cross-app Facebook signal channel, simultaneous use of all four Privacy Sandbox APIs, and a hardcoded Firebase key all correct to MEDIUM. Four form replies were received across 27 June to 13 July 2026, each repeating a redirect to trivago's third-party bug-bounty intake channel without addressing any specific finding; the final reply declared the matter closed on trivago's side. A 48-hour, finding-by-finding response deadline set on 10 July 2026 passed without any further reply of any kind.

ID	Severity	Title
C1	MEDIUM	A Native SDK Disguised as an Unrelated Vendor's Product, Three Layers of Obfuscation, Fires Before Consent
C2	MEDIUM	Firebase Remote Config Allows Post-Install Tracking Reconfiguration Without an App Update
H1	HIGH	Cleartext Traffic Permitted by Default on a Hotel-Search and Booking App
H2	HIGH	Production-Shipped Debug HTTP Interceptor Configured for Indefinite Log Retention
H3	MEDIUM	Undisclosed Facebook Cross-App Signal Channel
H4	MEDIUM	All Four Privacy Sandbox APIs Declared Simultaneously, Plus a Dedicated AppsFlyer Endpoint
M1	MEDIUM	Firebase API Key Hardcoded and Extractable

Subject & Operator Analysis

trivago is a hotel and travel price-comparison platform operated by trivago N.V., headquartered in Düsseldorf, Germany, placing the North Rhine-Westphalia data protection authority (LDI NRW) as lead supervisory authority.

Four Form Replies, One Redirect, One Self-Declared Closure, Then Silence

This case's correspondence record includes four inbound replies, not silence throughout, though none engaged the technical substance. On 27 June, 1 July, 10 July, and 13 July 2026, trivago's Zendesk-generated User Support desk replied each time with a close variant of the same message: the report had been forwarded internally for review, and trivago maintains a single intake channel for security and privacy submissions, its Vulnerability Disclosure Program on the third-party platform YesWeHack. None of the four replies addressed any of the six specific findings individually. On 10 July 2026, RFI-IRFOS set a 48-hour deadline for a named, dated, finding-by-finding response. trivago's reply on 13 July 2026, one day past that deadline, repeated the same VDP redirect and added that trivago considered the matter closed on its end. Two further messages, on 5 August and 6 September 2026, drew no reply of any kind.

Findings

C1: A Native SDK Disguised as an Unrelated Vendor's Product, Three Layers of Obfuscation, Fires Before Consent

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.

libakamaibmp.so, compiled for arm64, armeabi, x86, and x86_64, runs in an isolated process (:com.akamai.webview.process) and is branded in the manifest as an Akamai component. Independent analysis found this library actually corresponds to CyberfEnd, obscured behind three layers: runtime string decryption, a native binary resistant to static analysis, and a separately named process. It initializes at initOrder=100, before any consent mechanism can run.

```
libakamaibmp.so (arm64/armeabi/x86/x86_64), isolated process :com.akamai.webview.
    process
initOrder=100 (fires before consent)
Runtime string decryption via compiled decryption method (DBn-pattern), CyberfEnd
    identity confirmed beneath the Akamai branding
```

Impact: A tracking library's true vendor identity is actively obscured behind three independent layers, and it begins running before any consent mechanism, before a user has agreed to anything.

Fix: Disclose the library's actual vendor identity in the app's privacy documentation and defer its initialization until after consent. No confirmation that this has occurred was ever received.

C2: Firebase Remote Config Allows Post-Install Tracking Reconfiguration Without an App Update

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

Firebase Remote Config, confirmed via 57 compiled classes, allows trivago to change the app's tracking configuration after installation, invisibly to app-store review and to a user who consented to the app's data practices only at install time.

Impact: The app's actual tracking behavior can change at any time via a server-side push, outside app-store review and outside a user's original consent decision.

Fix: Disclose Firebase Remote Config's runtime-reconfiguration capability explicitly and commit to a change-notification process for material tracking updates. No confirmation that this has occurred was ever received.

H1: Cleartext Traffic Permitted by Default on a Hotel-Search and Booking App

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

android:cleartextTrafficPermitted is set to true as the app's base configuration, meaning unencrypted HTTP is permitted by default, not scoped to any specific legacy exception.

```
cleartextTrafficPermitted="true" (base configuration)
```

Impact: Hotel search queries and related account activity can transit in plaintext over an open or compromised network, such as public WiFi at the exact venues, airports and hotel lobbies, where this app is most often used.

Fix: Set cleartextTrafficPermitted to false globally and configure per-domain exceptions only where strictly necessary. No confirmation that this has occurred was ever received.

H2: Production-Shipped Debug HTTP Interceptor Configured for Indefinite Log Retention

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

ChuckerInterceptor is compiled into the production binary, configured with RetentionManager$Period.FOREVER, meaning intercepted API traffic is retained on-device indefinitely, not for a bounded debug window.

```
ChuckerInterceptor (production binary)
RetentionManager$Period.FOREVER (indefinite on-device log retention)
```

Impact: A debug HTTP logger shipped to production retains a full, indefinite on-device record of network traffic; if active, any party with local device access could read the complete captured history, not merely a recent debug window.

Fix: Confirm and strip Chucker and all debug-inspection tooling from production release builds via build-variant exclusion. No confirmation that this has occurred was ever received.

H3: Undisclosed Facebook Cross-App Signal Channel

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.

A Facebook PPML (Private Processing/Measurement Layer) IReceiverService is present, allowing Meta to receive cross-app signals without requiring direct user interaction with a Facebook-branded UI element.

Impact: Meta can receive behavioral signals from this app without a user-facing interaction that would make that data flow apparent.

Fix: Document the PPML integration explicitly under Art. 13(1)(e). No confirmation that this has occurred was ever received.

H4: All Four Privacy Sandbox APIs Declared Simultaneously, Plus a Dedicated AppsFlyer Endpoint

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.

All four Android Privacy Sandbox APIs (Topics, Attribution, Custom Audience, Ad ID) are declared simultaneously, alongside a dedicated AppsFlyer Privacy Sandbox endpoint (privacy-sandbox.appsflyersdk.com).

Impact: The full breadth of cross-app behavioral advertising infrastructure available on Android is active at once, with a dedicated third-party endpoint specifically built to consume it.

Fix: Document a specific legal basis for each Privacy Sandbox API in use, or reduce to only those with a disclosed purpose. No confirmation that this has occurred was ever received.

M1: Firebase API Key Hardcoded and Extractable

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

A Firebase API key is hardcoded and extractable from the production binary.

```
AIzaSyCywqj_Xjh8zzj5oaHfuIxUxeaG6iAp8nI
```

Impact: The key is trivially extractable, and depending on the security-rule configuration behind it, could enable unauthorized access or denial of service against legitimate users.

Fix: Restrict the Firebase API key by package name and SHA-1 certificate fingerprint. 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, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 7, Art. 25, Art. 13(1)(e)	C1	An obfuscated, vendor-disguised tracking library initializing before consent.
Art. 5(1)(a), Art. 13(1)(e)	C2	Post-install remote tracking reconfiguration outside app-store review.
Art. 32	H1	Cleartext traffic permitted by default on hotel-search and booking data.
Art. 32	H2	Production-shipped debug HTTP interceptor with indefinite log retention.
Art. 13(1)(e)	H3	Undisclosed Facebook cross-app signal channel.
Art. 5(1)(b), Art. 6(1)	H4	Simultaneous use of all four Privacy Sandbox APIs plus a dedicated attribution endpoint.
Art. 32	M1	Hardcoded, trivially extractable Firebase API key.

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. In this report, H1 and H2 reach HIGH on their computed CVSS v4.0 scores alone, no editorial escalation applied; C1, C2, H3, H4, and M1 correct to MEDIUM to match their own computed bands. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: TRIVAGO-2026-R1.