Coordinated Security & Privacy Disclosure, Final Report

VOL.at for Android (at.vol.android)

Seven written notices, ninety-one days, zero replies, zero bounces, zero automated acknowledgments of any kind

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – EIGHT FINDINGS ON VORARLBERG'S DOMINANT NEWS PORTAL, INCLUDING A CONCEALED-ORIGIN RUSSIAN SDK, TOTAL SILENCE

Target	Russmedia Digital, part of the Russmedia Gruppe, Vorarlberg, Austria, operator of VOL.at, described in RFI-IRFOS's own R1 as "Vorarlbergs dominantes Nachrichtenportal"
Product audited	VOL.at for Android, at.vol.android, v3.819
Disclosure reference	REF: at.vol.android
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (three CRITICAL findings, including a concealed-Russian -origin push SDK active on device boot, all CVSS v4.0 8.6-8.8, none reverified as remediated since 25 August 2026)

rfi.irfos@gmail.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of the production VOL.at Android application and identified eight findings: three hardcoded API keys (Firebase, Google Maps, YouTube) in the shipped APK, a global cleartext network security configuration permitting unencrypted HTTP for login, article, comment, and telemetry traffic, an active Pushwoosh (Arello Mobile) push-notification SDK registering on every device boot and transmitting device identifiers to Singapore, Russmedia's own debug-console overlay service left in the production build, a StartApp background service performing broad device-data collection compounding the cleartext exposure, a Facebook SDK with a broken login callback scheme enabling OAuth-callback hijacking by other apps on the same device, an undisclosed Swiss out-of-home advertising processor (APG|SGA), and Privacy Sandbox Topics API attribution left unrestricted alongside location and phone-state permissions exceeding VOL.at's own stated purpose for them.

Pushwoosh (Arello Mobile, headquartered in Novosibirsk with a Singapore presence) is a documented case: Reuters and the office of US Senator Ron Wyden reported in November 2022 that the vendor concealed its Russian origin for years, after which the US Army pulled its 'Army One' app and the CDC removed Pushwoosh from its published app list. VOL.at's production build registers com.pushwoosh.BootReceiver on every device restart across its entire reader base, transmitting push tokens and device identifiers to Singapore with no EU adequacy decision covering that transfer and no Art. 28 processor agreement disclosed.

This case is distinguished by the completeness of its silence: across seven written notices over ninety-one days, cc'd to the Austrian Datenschutzbehörde from 3 July 2026 onward, not one reply, bounce, or automated acknowledgment of any kind was ever received, a category of non-response RFI-IRFOS's own correspondence describes verbatim as 'nicht eine einzige Antwort, nicht einmal ein Bounce.' None of the three CRITICAL findings has been independently reverified as remediated since 25 August 2026; RFI-IRFOS's own 4 September 2026 notice explicitly marks their live status 'unverifiziert' pending a fresh binary diff.

Scope: Static analysis of the publicly downloaded production VOL.at Android APK (v3.819), on an authorized test device, only. No VOL.at account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to datenschutz@vol.at and digital@russmedia.com, cc datenschutz@russmedia.com, bcc dsb@dsb.gv.at and cert@cert.at. Across seven written notices over ninety-one days, not one reply, bounce, or automated acknowledgment of any kind was ever received on this thread, a completeness of silence distinct from every other case in this campaign, most of which produce at least an automated receipt.

ID	Severity	Title
CRITICAL-1	HIGH	Three hardcoded API keys in the public APK
CRITICAL-2	HIGH	Global cleartext traffic permitted for all connections

ID	Severity	Title
CRITICAL-3	HIGH	Pushwoosh, a concealed-Russian-origin SDK, active on every device boot
HIGH-1	MEDIUM	Russmedia's own debug-console overlay service shipped in production
HIGH-2	MEDIUM	StartApp SDK background service performing broad device-data collection
HIGH-3	MEDIUM	Facebook SDK: broken login callback scheme enables OAuth-callback hijacking
MEDIUM-1	MEDIUM	APG|SGA Connect SDK, undisclosed Swiss out-of-home advertising processor
MEDIUM-2	MEDIUM	Unrestricted Topics API attribution alongside location and phone-state permissions

Subject & Operator Analysis

Russmedia Digital, part of the Russmedia Gruppe based in Vorarlberg, Austria, operates VOL.at, described in RFI-IRFOS's own initial notice as Vorarlberg's dominant regional news portal, under the jurisdiction of the Austrian Datenschutzbehörde.

Findings

CRITICAL-1: Three hardcoded API keys in the public APK

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

res/values/strings.xml contains a Firebase key (AIzaSyA9PudAkJBtw6AESPEh3Vr4PgiQ_Xj7SVU), a Google Maps key (AIzaSyBxZrYVGiXr87DX_j_Q8mD6nx2gPiRuASI), and a YouTube key (AIzaSyAHoX4m1uCCUbhWkqndemCf-x33pAxL-DQ). The Firebase project is named 'volat---vorarlberg-online-app'; the triple-hyphen is a migration artifact indicating the credential lifecycle was never actively reviewed.

Confirmed unchanged as of the 4 September 2026 status check. No reply of any kind addressed this finding across seven notices.

Impact: Exposure spans quota/billing denial-of-service, forged push notifications, and unauthorized Maps/YouTube API usage billed against Russmedia's own project, across a dominant regional news portal's full reader base.

Fix: Rotate all three keys, apply API-level restrictions, and review the credential lifecycle that allowed a migration-artifact project name to ship to production.

CRITICAL-2: Global cleartext traffic permitted for all connections

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

The Network Security Config's base-config sets cleartextTrafficPermitted="true" globally, with no certificate pin configured. This affects login data, article requests, comment submissions, push-token registration, Facebook events, StartApp telemetry, and Pushwoosh device registration.

Never addressed in any reply across seven notices.

Impact: On an adjacent, attacker-controlled network, login credentials and the device-tracking data from every embedded SDK named in this report can be intercepted or manipulated in plaintext.

Fix: Remove the global cleartext exception, enforce TLS, and add certificate pinning for authentication and comment-submission endpoints.

CRITICAL-3: Pushwoosh, a concealed-Russian-origin SDK, active on every device boot

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

com.pushwoosh.BootReceiver registers on BOOT_COMPLETED, alongside LocalNotificationReceiver and NotificationUpdateReceiver. Pushwoosh is developed by Arello Mobile, headquartered in Novosibirsk, Russia, with a Singapore business presence; push tokens and device identifiers are sent to Singapore on every device restart.

Reuters and the office of US Senator Ron Wyden documented in November 2022 that Pushwoosh concealed its Russian origin for years; the US Army subsequently pulled its 'Army One' app and the CDC removed Pushwoosh from its published app list. No EU adequacy decision covers Singapore. Whether Russmedia's team was aware of this history, and whether a documented Art. 28 processor agreement exists with Arello Mobile, were asked repeatedly and never answered.

Impact: A device identifier and push-token stream from a dominant regional news portal's entire reader base reaches infrastructure tied to a vendor with a documented history of concealing its country of origin, with no disclosed transfer safeguard.

Fix: Remove Pushwoosh or obtain and publish a documented Art. 28 agreement and Art. 46 transfer mechanism for the Singapore-routed data, and disclose the processor relationship in the privacy policy.

HIGH-1: Russmedia's own debug-console overlay service shipped in production

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.3

com.russmedia.debugconsole.OverlayService, an in-house Russmedia developer tool rather than a third-party component, remains present and remotely activatable in the production build.

Never addressed in any reply.

Impact: A remotely-activatable in-house debug overlay left in a production release is an information-disclosure risk and a build-hygiene gap.

Fix: Strip debug-console components from the production build pipeline before release.

HIGH-2: StartApp SDK background service performing broad device-data collection

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

com.startapp.sdk.cachedservice.BackgroundService and com.startapp.sdk.jobs.SchedulerService run independently of app activity, historically collecting device IDs, installed-app lists, Wi-Fi SSID, and location.

Combined with CRITICAL-2, this data is transmitted unencrypted. Never addressed in any reply.

Impact: A background service independent of app activity broadens the device-data collection surface beyond what a news-reading app's stated purpose requires.

Fix: Restrict or remove the StartApp background service, and confirm any retained data collection is disclosed and purpose-limited.

HIGH-3: Facebook SDK: broken login callback scheme enables OAuth-callback hijacking

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 6.8

facebook_app_id 119571164772886 is paired with fb_login_protocol_scheme set to the literal placeholder "fb1234" instead of the correct "fb119571164772886", alongside AAM MetadataIndexer and AccessTokenManager$InstagramRefreshTokenInfo.

A placeholder callback scheme instead of the app-specific one means another app on the same device could register the same generic scheme and intercept the OAuth login callback. Never addressed in any reply.

Impact: A co-located malicious app registering the same placeholder URI scheme could intercept Facebook login callbacks intended for VOL.at.

Fix: Correct fb_login_protocol_scheme to the app-specific value (fb119571164772886) so the callback URI cannot be claimed by another app.

MEDIUM-1: APG|SGA Connect SDK, undisclosed Swiss out-of-home advertising processor

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

ch.apgsga.apgconnect.networking.NetworkService correlates mobile users with digital out-of-home advertising displays; APG|SGA is not named as a processor in the privacy policy.

Never addressed in any reply.

Impact: Mobile users are correlated with physical advertising displays through an undisclosed processor relationship.

Fix: Name APG|SGA explicitly as a processor in the privacy policy.

MEDIUM-2: Unrestricted Topics API attribution alongside location and phone-state permissions

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

ACCESS_ADSERVICES_TOPICS is set, ad-services-config.xml contains an unrestricted <attribution allowAllToAccess="true" />, and READ_PHONE_STATE plus ACCESS_FINE_LOCATION are both present. The app's own strings describe location use as limited to weather/news localization.

That stated purpose is exceeded by the simultaneously active StartApp, Facebook AAM, and APG|SGA components. Never addressed in any reply.

Impact: Location and device-identifier permissions granted for a narrow stated purpose are reachable by multiple third-party SDKs whose actual use exceeds that stated purpose.

Fix: Restrict Topics API attribution access, and confirm location/phone-state data is not reachable by SDKs beyond the app's own stated weather/news localization purpose.

A Case Defined by Total Silence

This case stands apart from most of this disclosure campaign not merely for receiving no substantive reply, but for receiving no response of any kind: no human reply, no automated ticket acknowledgment, no bounce, across all seven notices and ninety-one days. RFI-IRFOS's own correspondence tracked this explicitly, describing the state on 25 August 2026 as 'nicht eine einzige Antwort, nicht einmal ein Bounce' and on 4 September 2026 as unchanged. Because no reply or independent re-verification was ever received, none of the three CRITICAL findings' live status could be confirmed remediated between the 25 August 2026 status check and this report's publication; they are documented here as last verified on that date, not as of today.

Data Protection, Article by Article

Finding	Provision	Concern
CRITICAL-1	GDPR Art. 32(1)	Three hardcoded API keys, unaddressed
CRITICAL-2	GDPR Art. 32(1)(a), Art. 25	Global cleartext traffic, unaddressed
CRITICAL-3	GDPR Art. 46, Art. 13(1)(e)	Concealed-origin SDK routing device data to Singapore, no adequacy or Art. 28 agreement disclosed
HIGH-1	GDPR Art. 32(1), Art. 25	In-house debug overlay in production
HIGH-2	GDPR Art. 5(1)(c), Art. 13(1)(e), Art. 6(1)	Broad device-data collection exceeding stated purpose
HIGH-3	GDPR Art. 13(1)(e), Art. 46	Broken OAuth callback scheme, cross-app hijack risk
MEDIUM-1	GDPR Art. 13(1)(e)	Undisclosed out-of-home advertising processor
MEDIUM-2	GDPR Art. 5(1)(b), Art. 5(1)(c), TKG 2021 §165	Location/device permissions reachable beyond stated purpose

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to datenschutz@vol.at, digital@russmedia.com, cc datenschutz@russmedia.com, bcc dsb@dsb.gv.at, cert@cert.at; 3 CRITICAL + 3 HIGH + 2 MEDIUM findings disclosed; a paid remediation-engagement offer was also included in this and later notices, historical record only, not a currently open offer; embargo stated as 2026-09-19
2026-06-27	First follow-up, no regulator cc yet, no reply received
2026-07-03	Second follow-up, dsb@dsb.gv.at added to cc from this point onward
2026-07-17	Third follow-up, ’26 Tage Stille’, subject pivots to spotlight the Pushwoosh finding specifically
2026-07-27	Fourth follow-up, a 48-hour response deadline had lapsed 24 days prior, three questions repeated, escalation to the Datenschutzbehörde announced
2026-08-25	Fifth follow-up, ’65 Tage. Fünf Nachrichten.’, states explicitly that not one reply or bounce has ever been received
2026-09-04	Sixth follow-up, ’75 Tage. Sechs Nachrichten.’, sets a final deadline of 2026-09-11, marks all three CRITICAL findings ’unverifiziert’ pending a fresh diff; last message in the thread
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Rotate all three exposed API keys and review the credential-lifecycle process that let a migration-artifact project name ship to production.
- Remove the global cleartext exception and enforce TLS with certificate pinning for authentication and comment endpoints.
- Remove Pushwoosh or obtain and publish a documented Art. 28 agreement and Art. 46 safeguard for its Singapore-routed data.
- Strip the in-house debug-console overlay from the production build pipeline.
- Correct the Facebook SDK's login callback scheme to prevent cross-app OAuth-callback hijacking.
- Name APG|SGA explicitly as a processor and restrict Topics API attribution and location/phone-state access to the app's own stated purpose.

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. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 6, 13, 25, 32, 46. TKG 2021 §165. REF at.vol.android.