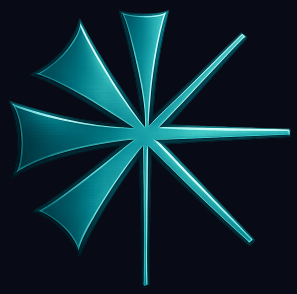

Wolt Android Apps

89-Day Disclosure Record

com.wolt.courierapp v2.184.0 & com.wolt.android v26.23.3 - an identity-token gap flagged in round one, still open at embargo.

EMBARGO REACHED 2026-08-23 - FINDING #11 STILL OPEN

Analyst	RFI-IRFOS Research Team
Report date	2026-08-23
Operator	Wolt Enterprises Oy (DoorDash, Inc. subsidiary)
First notified	2026-05-25 - ticket #INC-1994788
Rounds of contact	5 + 1 substantive reply (07-10)
Severity	1 CRITICAL (open) - 2 of 13 original findings confirmed fixed
Embargo	2026-08-23 - 90 days from first notification, computed once

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

Contents

1 Executive Summary 3

2 Subject & Operator Analysis 4

3 Architecture & Attack Surface 4

4 Findings 5
- 4.1 W-01: Iterable messaging runs without an identity token - original finding #11, still open . . . 5
- 4.2 W-02: Verbose networking and identifier logging in a release build . . . 5
- 4.3 W-03: Hardcoded San Francisco default map camera on every launch . . . 5
- 4.4 W-04: Location-polling volume consistent with reported battery drain . . . 6
- 4.5 W-05: Dead React-Native event wiring and two static nits (courier) . . . 6
- 4.6 W-06: WhatsApp OTP receiver exported without confirmed sender validation - consumer app . . . 6

5 The Complete Chain: Report to Unresolved Risk 6

6 Impact Analysis 7

7 Data Protection - Article by Article 7

8 Regulatory & Legal Landscape 8

9 Indicators of Compromise / Technical Summary 8

10 Disclosure Timeline & Outcome 9

11 Residual Risk & Recommendations 10

Executive Summary

On 2026-05-25, RFI-IRFOS reported thirteen security findings across Wolt's two Android applications, the courier app and the consumer app. Most operators in this position go quiet, or point toward a bug-bounty programme they have no intention of paying out against a disclosure that already happened for free. Wolt did neither. Its security team wrote back the same day, put a named contact behind the reply, and asked for something almost nobody in this disclosure programme asks for: a second, deeper audit once its next release had shipped.

RFI-IRFOS ran that second pass for free, live, on a real device, against a real courier session. Two of the original thirteen findings came back fixed. That is the part of this story that reads the way a disclosure is supposed to read: a report goes out, an engineer reads it, a build ships, a problem goes away.

The finding that mattered most did not go away. The courier app's messaging integration, Iterable, still opens the channel couriers depend on for delivery-relevant messages with no identity token attached to it, so the app itself has no way to confirm that a message arriving on that channel actually came from Wolt. It was true on 2026-05-25. It was still true when RFI-IRFOS went back and watched it happen live on 2026-06-14. It has been restated in three further rounds of contact since, and it is still true tonight, as the 90-day embargo on this disclosure closes.

What makes this worth reading past the technical detail is what sits right next to it. The consumer app, audited in the same pass on the same device, has none of this problem: certificate pinning enforced, keystore keys gated, nothing in cleartext, nothing leaking through debug logging. That is not a footnote to the finding above. It is the control group for it. It shows the gap on the courier side is not a capability Wolt lacks. It is a fix Wolt has, so far, chosen not to make.

Scope: Static root-level analysis (apktool, dex/string inspection, manifest review) of both published release APKs, plus live on-device dynamic analysis (adb logcat) during an active courier session. No production servers, backend infrastructure, or accounts were probed.

Disposition

Reported 2026-05-25, acknowledged the same day. Five rounds of contact over 90 days, one substantive reply on 2026-07-10 redirecting to a bug-bounty programme, one direct yes-or-no question left unanswered for 44 days. Embargo reached 2026-08-23. This is the first case in this programme where an operator engaged in good faith at every step and still let the finding that mattered go unfixed.

ID	Severity	Title
W-01	CRITICAL	Iterable messaging runs without an identity token - original finding #11, still open
W-02	MEDIUM	Verbose networking and identifier logging in a release build

ID	Severity	Title
W-03	MEDIUM	Hardcoded San Francisco default map camera on every launch
W-04	MEDIUM	Location-polling volume consistent with reported battery drain
W-05	LOW	Dead React-Native event wiring and two static nits (courier)
W-06	LOW	WhatsApp OTP receiver exported without confirmed sender validation - consumer app

Subject & Operator Analysis

Wolt Enterprises Oy is the operator of record for both apps, a Finland-headquartered food-delivery company that DoorDash acquired in 2022. Peel the Wolt branding off the courier app, though, and the code underneath is not really Wolt's own. It is DoorDash's Dasher driver platform, carried over almost untouched: the API still refers to a courier internally as a "Dasher," and the backend it talks to is still hosted at dashapi.com, DoorDash's own domain, four years after the acquisition closed. None of that is a finding by itself; companies inherit codebases after a merger all the time. But it changes what this report is actually about. Every gap documented here is not necessarily a Wolt-specific bug. It is a candidate to be sitting, just as unfixed, inside DoorDash's own driver fleet everywhere else the same platform runs.

Assessment

Of every operator in this disclosure programme, Wolt is the one that did almost everything right on the human side: a same-day reply, a named engineer, an invitation to look harder rather than an instinct to deflect. And the finding that mattered still did not get fixed. That is the more useful data point, not the less useful one. It means good faith on its own is not enough.

Architecture & Attack Surface

What actually broke is easy to describe, and on the evidence, easy to fix. Iterable, the SDK Wolt uses to send in-app messages and push notifications, is fully wired into the courier app and actively sending real messages to real couriers every working day. The only thing missing is the one line of code that would let it prove any of those messages are genuine.

```
Courier authenticates          -->  Wolt/DoorDash backend session established
        |
        v
RNIterableAPIModule.setUserId(riderID)      <- courier ID set
        |
        v
RNIterableAPIModule authToken: null          <- MISSING
        |
        v
Iterable in-app message / push channel       <- no verifiable binding to
                                                   the authenticated session
```

Because the token is missing rather than merely misconfigured, the app itself has no way to check that a message arriving through this channel actually came from Wolt's backend, for this courier, in this session. That was true in the original report. It was still true five weeks later, watched live on a device mid-shift. It has been true in every round of contact since. None of that needed a second audit to discover. It needed one commit to fix.

Findings

W-01: Iterable messaging runs without an identity token - original finding #11, still open

CRITICAL - Missing authentication (CWE-306)

The courier app's Iterable session initializes with the rider ID set but authToken left null - no identity binds the in-app messaging/push channel to the authenticated courier.

```
RNIterableAPIModule: setUserId: [rider-ID redacted at courier's request]  authToken:
    null
```

Impact: In-app message and push spoofing risk persists on a channel used for delivery-relevant communication. Unchanged since 2026-05-25 and the 2026-06-14 live re-confirmation.

Fix: Issue and set the Iterable JWT (authToken) per session.

W-02: Verbose networking and identifier logging in a release build

MEDIUM

WoltHeaderInterceptor logs every request line in full; a separate line records the courier's user ID in plaintext roughly 90 times per session.

```
Request: GET https://unified-gateway.dashapi.com/dasher-comms/v1/...
NetworkingDataModule: getAccessToken called - hasToken: true   (~90x/session)
```

Impact: Token values are no longer printed (fixed since the original finding #12), but internal API structure and identifiers remain readable via logcat with USB debugging enabled.

W-03: Hardcoded San Francisco default map camera on every launch

MEDIUM

Every launch briefly renders centered on DoorDash's home city before re-targeting to the courier's real location - a visible artifact of the shared DoorDash codebase.

```
DashCameraOptions FromLatLng(lat=37.774899, lon=-122.419400)  <- San Francisco (
    default)
DashCameraOptions FromLatLng(lat=47.069097, lon= 15.427488)   <- Graz (actual, ~15s
    later)
```

Impact: Minor UX defect; included as further evidence of the inherited-codebase reality described in Section 2.

W-04: Location-polling volume consistent with reported battery drain

---

MEDIUM

944 location callbacks were rejected by the OS as redundant in a single session, sub-meter and sub-second cadence.

Impact: Directly consistent with the battery drain and GPS ”stickiness” couriers report over a full shift.

Fix: Apply sane distance/time filters to the location request.

W-05: Dead React-Native event wiring and two static nits (courier)

LOW

76 unhandled bridge events per session; a hardcoded Google API key and an exported Compose preview activity remain in the release build.

Impact: Wasted bridge work and minor hygiene items, not independently exploitable.

W-06: WhatsApp OTP receiver exported without confirmed sender validation - consumer app

---

LOW

OtpCodeReceiver is exported to implement the WhatsApp OTP protocol; whether it verifies the broadcast actually originates from WhatsApp before accepting a code was not confirmed statically.

Impact: A malicious app could otherwise attempt to forge the broadcast.

The Complete Chain: Report to Unresolved Risk

Strip away the technical vocabulary and this is a simple story about time. A gap was found. A company was told. The company said yes, said thank you, asked to be checked again. It was checked again, and the same gap was still there. It was raised a third time, a fourth time, a fifth time. On the other end of every one of those messages was an operator that, by every visible sign, wanted to be seen doing the right thing, and never quite did the one thing that would have actually closed it.

Stage	Mechanism	Status at embargo
1. Root cause	Iterable initialized with authToken left null	Present since 2026-05-25
2. Live re-confirmation	Re-audited on-device, logcat-confirmed still null	Confirmed 2026-06-14
3. Engagement	Wolt's security team replies once, redirects to bug bounty	Reply 2026-07-10, no fix confirmation
4. Direct question	One yes/no asked: is #11 fixed	Unanswered since 2026-07-10
5. Final notice	Five days to embargo, question restated	Sent 2026-08-18, no reply
6. Embargo	90 calendar days from first notification	Reached 2026-08-23, gap open
7. Residual risk	No identity binding on courier messaging channel	Live and unresolved

Impact Analysis

For the couriers actually carrying this app through a shift, the open finding is not abstract. It sits on the exact channel Wolt uses to reach them with delivery-relevant messages, and because that channel carries no identity token, the app cannot tell a genuine message from a forged one arriving through the same pipe. These are workers paid by the delivery, not by the hour, for whom a spoofed message about a job is not a theoretical risk category. It is money and time. For the people using the consumer app, none of this applies; that side of the audit came back clean, which is precisely why it matters, because it proves the gap on the courier side is not something Wolt is incapable of closing. And for Wolt as a company, the lesson sits in between the two: acknowledgment is not remediation. A same-day reply and a named contact are worth something, more than most operators in this programme ever offer, but only a live re-test actually confirms a fix, and the live re-test found the gap exactly where it had been in May.

Data Protection - Article by Article

None of this happens in a vacuum. The data at stake, a courier's identity and the content of the messages sent to them about their own delivery work, is personal data, and Wolt is its controller under the GDPR. Three articles are directly engaged by what this audit found, not as abstract compliance language but because each one describes, almost exactly, the specific gap documented above.

Article	Obligation	How it is engaged
Art. 25	Data protection by design & default	Identity-token omission is a design gap present in every shipped build since the original report

Article	Obligation	How it is engaged
Art. 32(1)(b)	Integrity & confidentiality of processing	No verifiable binding between the authenticated courier session and the channel that communicates with them
Art. 5(2)	Accountability	No demonstration was offered in five rounds of contact that the gap does not affect message integrity

Regulatory & Legal Landscape

This report goes to three authorities in parallel, each for a different reason grounded in where it actually reaches. Austria, because the disclosure originated there and Austrian users of both apps are affected. Finland, because that is where Wolt Enterprises Oy is legally established, and where a lead-supervisory-authority role under Article 56 may ultimately sit. And the European Data Protection Supervisor, because DoorDash, the American parent now running the codebase underneath Wolt's own app, sits outside the reach of any single national authority acting alone. The following is analysis for the competent authorities, not a legal determination.

Authority	Jurisdictional hook	Potential basis
Osterreichische Datenschutzbehorde (DSB)	Austrian-initiated disclosure, AT users of both apps reached	GDPR Art. 5(2), 25, 32
European Data Protection Supervisor (EDPS)	Cross-border relevance: DoorDash, the non-EU parent, operates the shared codebase	Oversight coordination
Finnish Data Protection Ombudsman	Wolt Enterprises Oy is Finland-established	Possible Art. 56 lead-authority role, left to the regulator

Indicators of Compromise / Technical Summary

Type	Value
Courier package	com.wolt.courierapp v2.184.0
Consumer package	com.wolt.android v26.23.3
Affected SDK	Iterable (RNIterableAPIModule)
Root cause	authToken left null at session init
Backend (inherited)	dashapi.com - DoorDash Dasher platform

Type	Value
Operator	Wolt Enterprises Oy (DoorDash, Inc. subsidiary)
Ticket	#INC-1994788
First notified	2026-05-25
Embargo	2026-08-23 - 90 days, computed once

Disclosure Timeline & Outcome

Date	Event
2026-05-25	R1 sent, 13 findings. Same-day acknowledgment, ticket #INC-1994788 opened.
2026-06-14	R2 sent - live, on-device re-audit after Wolt asked for a deeper second look.
2026-06-27	Follow-up, 13 days since R2, no reply. Finding #11 restated.
2026-07-05	Third notice - 41 days since R1, 21 since R2, six days past a set deadline.
2026-07-10	Only substantive reply. Wolt redirects future findings to Intigriti. RFI-IRFOS declines same day, asks one direct yes/no on #11.
2026-08-05	Fourth notice, 26 days since the reply, question still unanswered.
2026-08-18	Fifth and final notice, five days to embargo, question restated once more.
2026-08-23	Embargo reached. No further reply since 2026-07-10. This report publishes as scheduled.

Outcome

Five rounds of contact. Ninety days. One substantive reply. One direct yes-or-no question, asked in writing on 2026-07-10, still unanswered forty-four days later. A company capable of replying the same day it first heard from RFI-IRFOS does not take forty-four days to answer yes or no by accident. No sixth message was sent chasing a reply that had, in every way that matters, already been declined by silence.

Residual Risk & Recommendations

Open

Finding W-01 is unresolved as of the embargo date. This report does not claim active exploitation was observed or attempted - no network interception, account compromise, or data exfiltration was performed at any point.

The fix itself is small: issue the Iterable session token the way every other authenticated call in this app already does, and W-01 closes. Given that the courier app is DoorDash's own Dasher platform underneath, the more consequential question is not really about Wolt at all. It is whether the same gap sits open, right now, across DoorDash's own driver fleet everywhere else that codebase runs, entirely apart from any Wolt branding. RFI-IRFOS did not audit that fleet and makes no claim about it beyond the question itself.

Both apps stay on RFI-IRFOS's weekly APK-diff schedule going forward: any silent patch, permission change, SDK swap, or endpoint change gets documented on the public record without reopening or extending this embargo. And if Wolt does eventually reply, whether that reply is a fix or a refusal, this record will be updated to say so, in either direction.

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 All findings derive from a real device (adb, live logcat, static apktool analysis of the pulled base.apk) plus written correspondence with Wolt's own security team. No network interception, account compromise, or data exfiltration was performed at any point. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF WOLT-2026.