Koordinierte Sicherheits- und Datenschutz-Offenlegung, Abschlussbericht

willhaben für Android (at.willhaben)

Zwölf schriftliche Benachrichtigungen, acht automatische Ticket-Antworten, eine inhaltsleere Weiterleitungsbestätigung, dann ein Portal-Verweis samt Rechtsdrohung wegen des Vergütungsmodells

ÖFFENTLICHE OFFENLEGUNG, 19. SEPTEMBER 2026 – SIEBEN BEFUNDE UNBEANTWORTET, KEINE TECHNISCHE STELLUNGNAHME ZU AUCH NUR EINEM PUNKT

Target	willhaben internet service GmbH & Co KG, Wien, Österreich
Geprüftes Produkt	willhaben für Android, at.willhaben, v8.48.0
Offenlegungsreferenz	REF WILLHABEN-2026-R1
R1 gesendet	2026-06-19
Offenlegungs-/Embargodatum	2026-09-19
Bericht veröffentlicht	2026-09-19
Schweregrad	HIGH (WH-05, Braze-Datentransfer österreichischer Nutzerdaten in die USA ohne konfigurierten EU-Endpunkt, CVSS v4.0 8.7, unbeantwortet)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

Am 19. Juni 2026 führte RFI-IRFOS eine statische Analyse der produktiven willhaben-Android-App durch und identifizierte sieben Befunde: drei fest kodierte Firebase-/Google-Schlüssel ohne Zertifikatsbeschränkung, ein OAuth-Redirect über ein Custom-Scheme ohne State-Parameter-Validierung, das durch jede installierte App abgefangen werden kann, ein ebenso abfangbares Zahlungsrückkehr-Scheme, fest kodierte Staging-Endpunkte und Test-Schlüssel im Produktions-Build, eine Braze-Konfiguration, die österreichische Nutzerdaten an ein US-Rechenzentrum sendet, obwohl ein EU-Endpunkt verfügbar wäre, kein Certificate Pinning auf API- und Zahlungsendpunkten, sowie vier fest kodierte Analytics-Zugangsdaten Dritter.

Über zwölf schriftliche Benachrichtigungen und acht automatische Ticket-Antworten hinweg antwortete am 8. Juli 2026 erstmals ein Mensch, eine generische Weiterleitungsbestätigung ohne jeden technischen Inhalt. Am 5. August 2026 antwortete das willhaben Security Team substanziell: es verwies auf sein eigenes Portal vdp.willhaben.at, bezeichnete RFI-IRFOS's NDA-Vergütungsmodell als 'rechtsmissbräuchliches Verhalten' und behielt sich rechtliche Schritte vor, sollte dieses 'Verhalten' nicht eingestellt werden. Kein einziger der sieben Befunde wurde dabei technisch benannt, bestätigt oder bestritten.

Nach dem 5. August 2026 kam keine weitere Nachricht von willhaben, trotz dreier weiterer schriftlicher Nachfragen. Die Fragen, ob eine interne Analyse des OAuth-Befunds (WH-02) erfolgt ist, ob eine Art.-33-DSGVO-Meldung an die Datenschutzbehörde vorbereitet wird, und auf welcher Rechtsgrundlage die Braze-Datenübermittlung in die USA erfolgt, blieben durchgehend unbeantwortet.

Scope: Statische Analyse der öffentlich über den Google Play Store bezogenen produktiven willhaben-Android-APK (v8.48.0), auf einem autorisierten Testgerät, ausschließlich. Es wurden keine willhaben-Konten, Backend-Systeme oder Infrastruktur zugegriffen oder getestet.

Disposition

R1 wurde am 19. Juni 2026 an datenschutz@willhaben.at gesendet. Über acht automatische Ticket-Antworten hinweg antwortete am 8. Juli 2026 erstmals ein Mensch, eine inhaltsleere Weiterleitungsbestätigung. Am 5. August 2026 antwortete das willhaben Security Team substanziell, verwies auf ein eigenes VDP-Portal, bezeichnete das NDA-Vergütungsmodell als rechtsmissbräuchlich und behielt sich rechtliche Schritte vor, ohne einen einzigen der sieben Befunde technisch zu kommentieren. Danach blieb jede weitere Nachricht unbeantwortet.

ID	Severity	Title
WH-01	HIGH	Drei fest kodierte Firebase-/Google-API-Schlüssel ohne Zertifikatsbeschränkung
WH-02	HIGH	OAuth-Redirect über Custom-Scheme ohne State-Parameter-Validierung

ID	Severity	Title
WH-03	MEDIUM	Zahlungsrückkehr-Scheme durch jede installierte App abfangbar
WH-04	MEDIUM	Staging-Endpunkte und Test-Registry-Schlüssel im Produktions-Build
WH-05	MEDIUM	Braze überträgt österreichische Nutzerdaten in die USA, obwohl ein EU-Endpunkt verfügbar wäre
WH-06	MEDIUM	Kein Certificate Pinning auf API- und Zahlungsendpunkten
WH-07	LOW	Vier fest kodierte Analytics-Zugangsdaten Dritter

Betreiberanalyse

willhaben internet service GmbH & Co KG betreibt Österreichs größten Online-Marktplatz, unter Aufsicht der österreichischen Datenschutzbehörde.

Findings

WH-01: Drei fest kodierte Firebase-/Google-API-Schlüssel ohne Zertifikatsbeschränkung

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

Drei separate Firebase-Projekte (whandroid-a3f05, whandroid-appsflyer, whandroid-appboy), keines mit Zertifikats-Fingerprint-Beschränkung in der GCP-Konsole, alle aus der öffentlichen APK extrahierbar.

Keine Reaktion von willhaben zu diesem oder irgendeinem anderen Befund auf technischer Ebene.

Impact: Drei Produktionsschlüssel bleiben ohne Nutzungsbeschränkung angreifbar.

Fix: Alle drei Schlüssel auf Paketnamen und Signaturzertifikat beschränken.

WH-02: OAuth-Redirect über Custom-Scheme ohne State-Parameter-Validierung

HIGH, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 8.5

RedirectActivity ist auf dem Custom-Scheme willhaben-app registriert, ohne android:autoVerify. Im Login-Flow wird der 'code'-Parameter für den Token-Austausch verwendet, PKCE ist vorhanden, aber keine State-Parameter-Validierung erfolgt vor dem Token-Austausch.

Jede auf dem Gerät installierte App kann dasselbe Scheme registrieren und den Redirect abfangen, was einen CSRF-artigen erzwungenen Login beziehungsweise eine Session-Übernahme ermöglicht. Keine technische Reaktion von willhaben.

Impact: Eine bösartige App auf demselben Gerät kann den Login-Flow kapern.

Fix: Einen kryptographisch zufälligen State-Parameter einführen und vor dem Token-Austausch validieren.

WH-03: Zahlungsrückkehr-Scheme durch jede installierte App abfangbar

HIGH, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 7.0

android:scheme="at.willhaben.mobileapp.paymentreturn" ist exportiert, ohne android:host-Attribut. Jede installierte App kann dasselbe Scheme registrieren und den Zahlungsbestätigungs-Callback abfangen.

Keine technische Reaktion von willhaben.

Impact: Zahlungsbestätigungsparameter können von einer bösartigen App auf demselben Gerät gelesen und manipuliert werden.

Fix: Ein App-Links-Verfahren mit android:autoVerify statt eines ungeschützten Custom-Schemes verwenden.

WH-04: Staging-Endpunkte und Test-Registry-Schlüssel im Produktions-Build

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

Drei Staging-API-Endpunkte und drei Test-Registry-Schlüssel sind im Release-Build fest kodiert.

Staging-Umgebungen weisen typischerweise schwächere Authentifizierung und ausführlichere Fehlermeldungen auf. Keine Reaktion von willhaben.

Impact: Entwicklungsinfrastruktur bleibt über den Produktions-Build erreichbar.

Fix: Staging-Konfiguration vollständig aus dem Produktions-Build-Flavor entfernen.

WH-05: Braze überträgt österreichische Nutzerdaten in die USA, obwohl ein EU-Endpunkt verfügbar wäre

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

Braze ist auf sdk.iad-01.braze.com (US East, Virginia) konfiguriert. Übermittelte Ereignisse umfassen 'Successful Sale', 'Email Request', 'Call', 'Login' und 'ApplyNow'. Braze bietet EU-Datenresidenz über sdk.fra-01.braze.com (Frankfurt) an; dieser Endpunkt ist nicht konfiguriert.

Auf welcher Art.-44-46-DSGVO-Transfergrundlage diese Übermittlung beruht und warum der verfügbare EU-Endpunkt nicht konfiguriert ist, wurde trotz wiederholter Nachfrage nie beantwortet.

Impact: Österreichische Nutzerdaten inklusive Verkaufsabschlüssen werden ohne erkennbaren Grund in die USA übertragen, obwohl eine EU-Alternative existiert.

Fix: Auf den Frankfurt-Endpunkt (sdk.fra-01.braze.com) umstellen.

WH-06: Kein Certificate Pinning auf API- und Zahlungsendpunkten

HIGH, CVSS v4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 7.1

network_security_config.xml deaktiviert Cleartext-Traffic korrekt global, enthält aber kein <pin-set> für api.willhaben.at oder die Paylivery-Zahlungsendpunkte.

Keine Reaktion von willhaben.

Impact: Stille TLS-Interzeption durch eine kompromittierte oder betrügerische CA bleibt möglich.

Fix: Certificate Pinning für alle API- und Zahlungsendpunkte implementieren.

WH-07: Vier fest kodierte Analytics-Zugangsdaten Dritter

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

Permutive-, Didomi- und Adjust-Zugangsdaten sind fest kodiert und ermöglichen das Vortäuschen von Ereignissen im Namen der willhaben-App.

Keine Reaktion von willhaben.

Impact: Drittanbieter-Analytics-Zugangsdaten ermöglichen Event-Spoofing.

Fix: Zugangsdaten rotieren und auf serverseitige Vermittlung umstellen, wo möglich.

Ein Portal-Verweis und eine Rechtsdrohung, keine technische Stellungnahme

Das willhaben Security Team antwortete am 5. August 2026 wörtlich: ”Meldungen zu möglichen Schwachstellen sind ausschließlich über das von uns hierfür vorgesehene Portal vdp.willhaben.at nach den von uns festgelegten Bedingungen zulässig.” Weiter: ”Darüber hinaus entnehmen wir Ihren bisherigen Mails, dass Sie für die von Ihnen mitgeteilten Informationen Entgelt für die Geheimhaltung (’NDA’) verlangen - nach unserem Rechtsverständnis handelt es sich dabei zumindest um rechtsmissbräuchliches Verhalten. Wir behalten uns jedenfalls rechtliche Schritte vor.” Keiner der sieben Befunde wurde in dieser oder einer späteren Nachricht technisch benannt, bestätigt oder bestritten. RFI-IRFOS’s Antwort vom selben Tag stellte klar, dass die Offenlegung unabhängig von jeder Zahlung fortgesetzt wird, wie bereits in R1 festgehalten. Danach kam keine weitere Nachricht von willhaben.

Datenschutz, Artikel für Artikel

Befund	Bestimmung	Anliegen
WH-01	DSGVO Art. 25(1), Art. 32(1)(b)	Fest kodierte Credentials ohne Beschränkung
WH-02	DSGVO Art. 32(1)(a); RFC 6749/6819	OAuth-Redirect ohne State-Validierung
WH-03	DSGVO Art. 32(1)(a)	Abfangbares Zahlungsrückkehr-Scheme
WH-05	DSGVO Art. 44-46	US-Datentransfer ohne genutzten EU-Endpunkt
WH-06	DSGVO Art. 32(1)(a)	Kein Certificate Pinning

Datum	Ereignis

Offenlegungsverlauf & Ergebnis

Datum	Ereignis
2026-06-19	R1 gesendet an datenschutz@willhaben.at, sieben Befunde
2026-07-08	Erste menschliche Antwort: inhaltsleere Weiterleitungsbestätigung (’Sandor’)
2026-08-05	willhaben Security Team: Portal-Verweis, Rechtsmissbrauchsvorwurf, Rechtsschritte vorbehalten, keine technische Stellungnahme
2026-08-12 / 08-18 / 09-04	Drei weitere Nachfragen, unbeantwortet
2026-09-19	Embargo, wie in den zuletzt gesendeten Nachrichten bestätigt, endet und dieser Bericht wird veröffentlicht

Restrisiko & Empfehlungen

- Den OAuth-State-Parameter (WH-02) einführen, bevor ein Login-Flow-Hijack real ausgenutzt wird.
- Auf den verfügbaren EU-Braze-Endpunkt umstellen (WH-05).
- Certificate Pinning auf allen API- und Zahlungsendpunkten implementieren (WH-06).

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 Koordinierte Offenlegung gemäß ISO/IEC 29147. Die Forschungstätigkeit ist durch das österreichische Forschungsfreiheitsgesetz (Art. 17 StGG) geschützt. DSGVO Art. 25, 32, 44-46. REF WILLHABEN-2026-R1.