# Security & Privacy Disclosure, Final Report

## 1Password for Android (com.onepassword.android)

Root level code analysis of the password-manager category, correspondence through 21 November 2026.

**PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. EMBARGO 21 NOVEMBER 2026. SECURITY TEAM ANSWERED IN PART, NO REPLY FROM THE PRIVACY TEAM.**

| | |
|---|---|
| **Target** | AgileBits Inc. (dba 1Password), 4711 Yonge St, 10th Floor, Toronto, Ontario, M2N 6K8, Canada |
| **Versions Audited** | 8.12.33 / 81233002 (23 Aug 2026, original notice) · 8.12.42 and 8.12.44 (28 Oct / 10 Nov 2026, re-pulled in correspondence) |
| **Notice / Publication** | 2026-08-23 / 2026-11-21 (90 days, unchanged) |
| **Findings** | 7: 0 High, 4 Medium, 3 Low |
| **Status** | SUBSTANTIVE, PARTIAL: Security team answered between 27 Oct and 17 Nov, one point conceded on each side, Privacy team (Sentry/GDPR/Art.27) silent since 28 Oct, no message after 17 Nov 2026 |
| **SHA-256 (base APK)** | `6ad64b9ecf07361ef412fe2f8704fe2f53f11386cb84928f61fc725be963cd69` |

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

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

## Contents


**1 Executive Summary** 3

**2 Finding Status at a Glance** 5

**3 Subject & Operator Analysis** 6

**4 Architecture & Data Flow** 6

**5 Findings** 7

5.1 H1: Network security config trusts user-installed CAs on account-authentication and sync domains; no certificate pinning . . . . . 7

5.2 M1: Crash/performance telemetry SDK initializes pre-consent; auto-collection scope unverified, routed to the Privacy team and unanswered . . . . . 8

5.3 M2: Hardcoded Firebase and Google Maps/Places API keys; server-side restriction asserted but not confirmed; manifest auto-init flag overridden in code 9

5.4 M3: No EU Art. 27 representative identified for Canada-headquartered operator; routed to Privacy team, unanswered . . . . . 10

5.5 L1: QUERY_ALL_PACKAGES: full installed-app visibility, no demonstrated transmission path . . . . . 10

5.6 L2: Internal dev/test backend domains exposed in production App Links manifest 11

5.7 L3: "Everyone" content rating on a billing-enabled credential/identity-document manager . . . . . 11

**6 Impact Analysis** 12

**7 The Complete Chain** 12

**8 Data Protection: Article by Article** 13

**9 Regulatory & Legal Landscape** 13

**10 Indicators of Compromise & Reproducible Evidence** 13

**11 Disclosure Timeline & Outcome** 14

**12 What 1Password Got Right** 15

**13 Residual Risk & Recommendations** 15

## Executive Summary

1Password for Android (com.onepassword.android) is AgileBits Inc.'s client for its password and identity management service, with an "Everyone" content rating, from a company that reports more than 200,000 business customers (1Password press release, 22 October 2026). On 23 August 2026 RFI-IRFOS disclosed seven findings from a root level code analysis of version 8.12.33 under REF 1PASSWORD-2026-R1. The two most consequential concerned a network security configuration that trusts user-installed certificate authorities on the exact domains carrying account authentication and sync traffic, and a crash/performance SDK that starts at process start behind a server feature flag, with no read of a consent decision found on that path. H1 was lowered from High to Medium on 17 November 2026 after 1Password explained the design in writing.

1Password's security team engaged substantively from 27 October 2026 onward, after an initial automated reply misdirected the notice to its HackerOne bug-bounty scope determination. The exchange narrowed to a documented disagreement rather than a silent dispute: 1Password confirmed in writing that trusting user-installed CAs on 1password.com/.ca/.eu is a deliberate design decision, published in its own Security Design White Paper, intended to let the app function inside managed (MDM) environments that inspect TLS, and backed by a compensating control (passkey and SSO credential bundles are encrypted with a device key that never leaves the device, independent of TLS). RFI-IRFOS records this as a documented, reasoned trade-off, not a silent gap, and treats the underlying question as answered in this report.

The harder disagreement sits on the two hardcoded API keys. 1Password's position is that a Firebase Cloud Messaging key is not meant to be secret by design. RFI-IRFOS's question was never about secrecy but about server-side restriction (App Check, Security Rules, API scoping), and 1Password's own written reply states that access is "controlled server-side" without naming which controls are in place, which this report records as an unconfirmed assertion rather than a resolved finding. In the same exchange, RFI-IRFOS traced the app's start sequence across versions 8.12.42 and 8.12.44 and found that Firebase Cloud Messaging auto-initialization is set to true in code at every cold start when Google Play Services is available, overriding the firebase_messaging_auto_init_enabled=false manifest flag the original notice had credited as a genuine privacy control. That credit is withdrawn in this report.

1Password's crash-reporting and EU-representative questions, both routed to privacy@1Password.com at 1Password's own request on 27 October 2026, remain unanswered as of 21 November 2026, twenty-four days after privacy@1Password.com was copied on 28 October 2026. The report below states what is demonstrated from the binary, what 1Password has confirmed in writing, what remains a documented disagreement, and what has gone twenty-four days without any answer from the team 1Password itself named as the right recipient.

**Scope:** Root level code analysis of the Google Play release binary 8.12.33 (versionCode 81233002, base.apk SHA-256 above), with classes.dex and classes2.dex fully disassembled at smali level (23,948 classes) and classes3.dex/classes4.dex reviewed via dex-string extraction only. Re-pulled and diffed against versions 8.12.42 and 8.12.44 during correspondence (27 October and 10 November 2026). No account was created beyond a standard trial sign-up, no backend was probed, no key was tested against a live server, and the native Rust crypto core (libop_core_android.so) was not reverse-engineered.

| ID | Severity | Title |
|---|---|---|
| H1 | MEDIUM | Network security config trusts user-installed CAs on account-authentication and sync domains; no certificate pinning |
| M1 | MEDIUM | Crash/performance telemetry SDK initializes pre-consent; auto-collection scope unverified, routed to the Privacy team and unanswered |
| M2 | MEDIUM | Hardcoded Firebase and Google Maps/Places API keys; server-side restriction asserted but not confirmed; manifest auto-init flag overridden in code |
| M3 | MEDIUM | No EU Art. 27 representative identified for Canada-headquartered operator; routed to Privacy team, unanswered |
| L1 | LOW | QUERY_ALL_PACKAGES: full installed-app visibility, no demonstrated transmission path |
| L2 | LOW | Internal dev/test backend domains exposed in production App Links manifest |
| L3 | LOW | ”Everyone” content rating on a billing-enabled credential/identity-document manager |

| ID | Disclosed | This report | Status as of 21 November 2026 |
|---|---|---|---|

## Finding Status at a Glance

| ID | Disclosed | This report | Status as of 21 November 2026 |
|---|---|---|---|
| H1 | HIGH | MEDIUM | Design decision confirmed in writing (27 Oct, 10 Nov), compensating controls named and recorded by RFI-IRFOS as a documented trade-off. Question closed. Lowered from High to Medium on 17 November 2026. |
| M1 | MEDIUM | MEDIUM | Unanswered. Routed to privacy@1Password.com on 28 October 2026 at 1Password's own request. On 17 November 2026 the security team wrote that the concerns were forwarded to internal departments. No reply from the privacy team as of 21 November 2026. |
| M2 | MEDIUM | MEDIUM | Disputed. 1Password states on 10 and 17 November that access is server-side controlled and not published, and will not name the controls (App Check, Security Rules, API restriction). Recorded as unconfirmed, not resolved. New sub-finding raised in correspondence: FCM auto-init overrides the manifest flag originally credited as a positive. |
| M3 | MEDIUM | MEDIUM | Unanswered. Routed to privacy@1Password.com on 28 October 2026. No reply as of 21 November 2026. |
| L1 | LOW | LOW | Not raised in correspondence; stands as disclosed, capability-only. |
| L2 | LOW | LOW | Not raised in correspondence; stands as disclosed, capability-only. |
| L3 | LOW | LOW | Not raised in correspondence; informational observation, stands as disclosed. |

## Subject & Operator Analysis

AgileBits Inc., doing business as 1Password, is headquartered at 4711 Yonge St, 10th Floor, Toronto, Ontario, Canada, per its own published privacy policy, which names AgileBits as controller and describes GDPR-relevant obligations without naming an Art. 27 EU representative anywhere in the text reviewed. The company has a HackerOne-hosted bug bounty program that its automated support channel initially applied to this notice, incorrectly, since the notice was sent directly to security@agilebits.com under RFI-IRFOS's standing process and was never filed through HackerOne. 1Password's security team corrected this on 27 October 2026, sixty-five days after the original notice, and engaged on the substance from that date.

## Architecture & Data Flow

1Password's Android client is a Kotlin/Java application with a 117 MB native Rust library, libop_core_android.so, that implements the crypto/sync engine entirely outside the reviewable managed-code layer. The app's sign-in model (ApiSignInWithPasswordAndSecretKeyRequest, PasswordAndSecretKeyCredentials) is architecturally consistent with 1Password's publicly documented Account Password plus Secret Key design. Account authentication and sync traffic route to 1password.com, 1password.ca and 1password.eu, with a dedicated EU backend domain (env_deu_domain) referenced in the manifest alongside the production EU host. A Sentry crash and performance SDK, bundled with screenshot-capture and session-replay-capable modules, initializes via an androidx.startup ContentProvider at process creation, structurally before any Activity including a first-run consent screen, though a genuine per-crash Send/Don't Send/Always Send dialog exists downstream of that initialization.

## Findings

### H1: Network security config trusts user-installed CAs on account-authentication and sync domains; no certificate pinning

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), lowered from HIGH on 17 November 2026 after the operator confirmed a deliberate design decision (27 October and 10 November 2026)**

RFI-IRFOS severity change: lowered from HIGH to MEDIUM/6.3 on 17 November 2026. The HIGH rating in the R1 rested on the channel carrying a Secret Key exchange. 1Password showed that no Secret Key is transmitted there, and RFI-IRFOS withdrew that wording on 28 October 2026. Blast-radius check of 17 November 2026: 1Password reports more than 200,000 business customers (1Password press release, 22 October 2026), which raises the consequence of an exploit. It does not offset the precondition of an installed certificate authority, the operator's written mitigation and the documented purpose of the design for managed environments. No upward adjustment applies.

```
<network-security-config>
    <base-config cleartextTrafficPermitted="true">
        <trust-anchors>
            <certificates src="system" />
            <certificates src="user" />
        </trust-anchors>
    </base-config>
    <domain-config cleartextTrafficPermitted="false">
        <domain includeSubdomains="true">1password.com</domain>
        <domain includeSubdomains="true">1password.ca</domain>
        <domain includeSubdomains="true">1password.eu</domain>
    </domain-config>
</network-security-config>
```

No CertificatePinner class exists in any of the four dex files (grep returned zero hits), and the native layer ships librustls_platform_verifier-*.so, which verifies against the OS/platform trust store rather than a fixed pin set.

1Password's written reply of 27 October 2026, quoting its own Security Design White Paper: "Neither certificate pinning nor DNSSec have been implemented... the marginal gain in security provided by such measures isn't something we consider to be worth the risk of availability loss should those extra measures fail in some way." Its reply of 10 November 2026 adds: trusting user-installed CAs for these domains is deliberate so that "1Password work[s] in managed environments that inspect TLS traffic," and an attacker who intercepts TLS during passkey or SSO sign-in receives a credential bundle "encrypted with a device key that never leaves the device." Password-based sign-in continues to rely on SRP (Secure Remote Password), under which, per the White Paper, "the verifier is the only sensitive information ever transmitted, and it's sent only during initial registration."

RFI-IRFOS's original notice referred to this channel as carrying the Secret Key exchange; 1Password correctly pointed out the Secret Key itself is never transmitted over the network, and RFI-IRFOS withdrew that specific wording in writing on 28 October 2026. The HIGH rating of the R1 depended on it, and the rating is lowered accordingly. The device key statement

of 10 November 2026 was not independently verified, and the native cryptographic core was not reverse-engineered.

**Impact:** A device with an attacker-installed or MDM-pushed certificate authority can intercept TLS on the channel carrying account-authentication and sync traffic, including the encrypted passkey/SSO credential bundle and the SRP verifier exchange, on every device where such a certificate authority is installed.

**Fix:** 1Password states the design is deliberate and names compensating controls (device-key encryption of the credential bundle, SRP for password sign-in). No change was committed in correspondence, and none is requested here; the finding is recorded as a disclosed, documented trade-off rather than an open defect.

**M1: Crash/performance telemetry SDK initializes pre-consent; auto-collection scope unverified, routed to the Privacy team and unanswered**

---

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), timing/consent-sequencing finding, not a confidentiality breach**

A Sentry crash and performance SDK ships classes for automatic breadcrumb collection, ANR profiling, and screenshot capture/session replay (io.sentry.android.replay.*, ScreenshotEventProcessor, ComposeViewHierarchyExporter). It initializes via androidx.startup's InitializationProvider ContentProvider at process creation, structurally before any Activity can render, including a first-run consent screen. A genuine per-event CrashReportAlert dialog (Send/Don't Send/Always Send) exists downstream, which this report credits as a real mitigation on the crash-report path specifically.

What could not be resolved statically, because the SentryAndroidOptions configuration call site sits inside heavily R8-minified code, is whether breadcrumb, ANR and performance telemetry are collected or transmitted independently of the per-crash dialog, and whether the bundled screenshot/session-replay modules are active or dormant in production.

1Password's written reply of 27 October 2026 states plainly that this is a privacy question, not a security one, and should be sent to privacy@1Password.com. RFI-IRFOS copied that address starting 28 October 2026. As of 21 November 2026, twenty-four days later, no reply has arrived from 1Password's Privacy team. On 17 November 2026 the security team wrote that the concerns were forwarded to internal departments.

**Fix:** Open. Routed to 1Password's own named recipient (privacy@1Password.com) on 28 October 2026, unanswered as of this report.

### M2: Hardcoded Firebase and Google Maps/Places API keys; server-side restriction asserted but not confirmed; manifest auto-init flag overridden in code

**LOW, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 1.8 (CVSS-B), rated MEDIUM by blast-radius escalation, server-side controls asserted by the operator but not confirmed**

RFI-IRFOS blast-radius escalation: raised from LOW/1.8 to MEDIUM because 1Password reports more than 200,000 business customers (1Password press release, 22 October 2026) and, as of 21 November 2026, 1Password's own written replies assert server-side restriction without naming which controls (App Check, Firebase Security Rules, API scoping) are actually in place, leaving the burden of proof unmet rather than discharged.

```
<string name="google_api_key">AIzaSyDlgdc49IyJVkVM67gEcQdckhwmgOe3Hz0</string>
<string name="google_app_id">1:928673166066:android:32ae1f1b58289ae669d66b</string>
<string name="gcm_defaultSenderId">928673166066</string>
<string name="google_storage_bucket">b5-notification-prd.appspot.com</string>
<string name="project_id">b5-notification-prd</string>
<string name="default_web_client_id">928673166066-8m4b8g2vce26qrl3m5giat1rhp0rkueb.
    apps.googleusercontent.com</string>
<meta-data android:name="com.google.android.geo.API_KEY" android:value="
    AIzaSyA4l7AU5a8YVkjwmJDmxRtl78lVWodnFoo"/>
```

Unchanged across 8.12.33, 8.12.42 and 8.12.44, confirmed by RFI-IRFOS re-pulling the binary on 10 November 2026.

1Password's 27 October reply: "These are client identifiers. They are meant to ship inside the package." Its 10 November reply quotes its own bug-bounty policy on the Firebase key ("This API key is intended to be exposed publicly... Unlike how API keys are typically used, API keys for Firebase services are not used to control access to backend resources") and states, for both keys and the storage bucket, "access is controlled server-side, and we don't share details of that internal configuration."

RFI-IRFOS's 10 November reply noted that the policy page 1Password cites itself states that Firebase-provisioned keys are "automatically restricted to Firebase-related APIs" and that the Maps/Places key is not Firebase-provisioned, so that specific restriction does not apply to it; and that access to backend resources is in fact governed by Firebase Security Rules and Firebase App Check per the same page, which 1Password's reply named without confirming either is enforced for this project.

New sub-finding, raised in correspondence and not in the original notice: tracing the app's start sequence in 8.12.42 and 8.12.44 (code identical in both) shows Application.onCreate sets Firebase Cloud Messaging auto-init to true whenever Google Play Services is available, which overrides the manifest's firebase_messaging_auto_init_enabled=false flag. RFI-IRFOS's original notice credited that flag as a genuine opt-in control (see WHAT YOU GOT RIGHT); that credit is withdrawn in this report. The traffic this triggers was not observed; this is a code-level override, not a demonstrated transmission.

**Impact:** A key with no confirmed server-side restriction in the binary of a password manager with more than 200,000 business customers carries a real, if unquantified, quota/billing-exhaustion and unauthorized-API-use exposure; the Firebase Cloud Messaging auto-init override means registration against google_api_key begins regardless of the manifest flag a user or auditor would otherwise read as an opt-in control.

**Fix:** Open. 1Password states access is server-side controlled; this report asks for the specific control (App Check enforcement status, Security Rules scope) in writing, not a restatement of the assertion.

**M3: No EU Art. 27 representative identified for Canada-headquartered operator; routed to Privacy team, unanswered**

---

**MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), transparency finding, routed and unanswered**

The app's manifest declares a dedicated EU-region backend domain (env_deu_domain = b5dev.eu, referenced alongside the production 1password.eu host), confirming EU-resident traffic is routed to EU-specific infrastructure. AgileBits Inc.'s published privacy policy (1password.com/legal/privacy) names AgileBits as controller at its Toronto address and states GDPR-relevant obligations, but names no Art. 27 EU representative anywhere in the text reviewed.

Routed to privacy@1Password.com on 28 October 2026 at 1Password's own direction. No reply as of 21 November 2026.

**Fix:** Open, unanswered.

**L1: QUERY_ALL_PACKAGES: full installed-app visibility, no demonstrated transmission path**

---

**LOW, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), capability-only, not raised in correspondence**

QUERY_ALL_PACKAGES grants visibility into every app installed on the device. No analytics, attribution, or telemetry SDK capable of receiving or transmitting an installed-package list was found anywhere in the binary (the SDK inventory is limited to Firebase-FCM, Sentry, Google Maps/Places, and ML Kit). Stated as a capability-without-demonstrated-transmission observation.

**Impact:** None demonstrated; capability exists but no transmission path was found.

**Fix:** Not raised in correspondence; stands as disclosed.

### L2: Internal dev/test backend domains exposed in production App Links manifest

**LOW, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), information-disclosure/attack-surface observation**

Four non-production hosts (b5dev.com, b5dev.ca, b5dev.eu, b5test.com) are declared in the same autoVerify="true" App Links intent-filter as the production 1password.com domain, confirming the internal project codename ("B5") and environment topology. These apex domains are not covered by the network_security_config.xml domain-config that disables cleartext for 1password.com/.ca/.eu, so any traffic directed to them would fall under the cleartext-permitted base-config. No evidence the app actively connects to these hosts in production.

**Impact:** Information-disclosure and attack-surface minimization observation; no demonstrated data exposure.

**Fix:** Not raised in correspondence; stands as disclosed.

### L3: "Everyone" content rating on a billing-enabled credential/identity-document manager

**LOW, CVSS v4.0 AV:N/AC:N/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), informational**

Play Store content rating: Everyone. The app requires com.android.vending.BILLING (paid subscription, no ad-supported free tier) and stores financial and identity-document-adjacent data by design. No age gate, date-of-birth field, or parental-consent string was found. Named explicitly per standing methodology rather than silently skipped; not itself unusual for a security/productivity tool, and a billing requirement is a soft adult-oriented gate.

**Impact:** Informational.

**Fix:** Not raised in correspondence; stands as disclosed.

## Impact Analysis

The population most exposed by H1 is 1Password's own stated target market for managed deployment: employees on enterprise MDM-enrolled devices, whose employer already has the technical means to install a trusted CA, and anyone whose device has been compromised to the point an attacker can push a CA without root. For that population, a TLS interception during passkey or SSO sign-in yields an encrypted credential bundle, not vault plaintext, per 1Password's own documented compensating control. M2's exposure is different in kind: the binary of a password manager with more than 200,000 business customers ships a key with an asserted but unconfirmed server-side restriction, and the Firebase Cloud Messaging auto-init override discovered in correspondence means registration traffic begins at every cold start regardless of the manifest flag a careful user or auditor would read as an opt-in control. M1 and M3 are pure transparency gaps: a user cannot know, from any document reviewed, what Sentry collects before the crash dialog appears, or who to contact in the EU under Art. 27, and both questions have sat unanswered with 1Password's own named Privacy team for twenty-four days as of 21 November 2026.

## The Complete Chain

Point of contact: a user installs 1Password from the Google Play Store, a password manager used by more than 200,000 businesses, and either signs up fresh or signs in with Account Password and Secret Key. Processing: on every cold start, before any screen renders, the app's androidx.startup ContentProviders fire, including the Sentry crash/telemetry initializer and, per the correspondence-sourced sub-finding, a Firebase Cloud Messaging auto-init call that fires regardless of the manifest's declared opt-in flag. Transport: account-authentication and sync traffic, including the SRP verifier exchange and, for passkey/SSO users, an encrypted credential bundle, travels over a channel whose base trust configuration accepts user-installed CAs, a configuration 1Password confirms is deliberate for MDM compatibility. Consequence if realized: an attacker or employer with CA-install capability on the device can observe traffic shape and metadata on that channel; per 1Password's own compensating control, the passkey/SSO credential bundle itself stays encrypted with a device key that never leaves the device, and password-based sign-in relies on SRP rather than TLS secrecy for its core security property. Residual exposure: the Firebase and Maps/Places keys sit in the binary with an operator assertion of server-side control that remains unconfirmed, and the Sentry pre-consent collection scope and EU representative questions remain open with no reply from 1Password's own named recipient.

## Data Protection: Article by Article

- Art. 7(1): whether Sentry's automatic breadcrumb, ANR and performance telemetry is collected before any consent decision is a live, unanswered question as of 21 November 2026 (M1).
- Art. 25: data protection by design is engaged by the Firebase Cloud Messaging auto-init override discovered in correspondence, which runs regardless of the manifest's own declared opt-in flag (M2).
- Art. 27: no EU representative has been identified for AgileBits Inc., a Canada-headquartered controller with a dedicated EU backend domain; the question has been with 1Password's Privacy team, unanswered, since 28 October 2026 (M3).
- Art. 32(1)(a)/(b): the network security configuration's acceptance of user-installed CAs on authentication/sync domains, and the unconfirmed server-side restriction on the Firebase and Maps/Places keys, both engage the appropriate-technical-measures and availability/resilience standards, with 1Password's position recorded for each (H1, M2).

## Regulatory & Legal Landscape

AgileBits Inc. is a Canada-headquartered controller offering services to EU data subjects. Absent a confirmed EU main establishment, a disclosure of this kind is addressed to the Austrian Datenschutzbehoerde (DSB) per RFI-IRFOS's standing practice, which copied the DSB and the European Data Protection Supervisor on the original notice. 1Password's own HackerOne bug-bounty program covers technical security submissions but, per its own 27 October reply, routes privacy-specific questions (consent timing, Art. 27 representation) to a separate Privacy team at privacy@1Password.com, which has not responded in this case as of 21 November 2026.

## Indicators of Compromise & Reproducible Evidence

| Artifact | Value |
|---|---|
| Package | com.onepassword.android |
| Base APK SHA-256 (8.12.33) | 6ad64b9ecf07361ef412fe2f8704fe2f53f11386cb84928f61fc725be963cd69 |
| Base APK SHA-256 (8.12.42, cited 28 Oct 2026) | 1f85e687e2fe2d5c0f1d1f6b380bc582390e5e4e68c08ead59af2575887e39ba |
| Base APK SHA-256 (8.12.44, cited 10 Nov 2026) | 1b8fb6767bd9282e7ff317219f063d6f5e78e676e5bbe6960ac71ede5366e6c2 |
| Firebase API key | AIzaSyDlgdc49lyJVkVM67gEcQdckhwmgOe3Hz0 |
| Firebase project | b5-notification-prd (app ID 1:928673166066:android:32ae1f1b58289ae669d66b, sender ID 928673166066) |

| Artifact | Value |
|---|---|
| Google Maps/Places key | AIzaSyA4l7AU5a8YVkjwmJDmxRtl78lVWodnFoo |
| Dev/test hosts in production manifest | b5dev.com, b5dev.ca, b5dev.eu, b5test.com |

## Disclosure Timeline & Outcome

23 August 2026: original notice to security@agilebits.com, four findings and three questions, 90-day embargo starts. 8 September 2026: automated reply misapplies HackerOne scope rules to a notice that was never filed through HackerOne; RFI-IRFOS corrects this the same day and restates the three questions, unanswered. 27 October 2026, sixty-five days later: 1Password's security team gives the first substantive reply, answering certificate pinning and the API keys from public documentation, and redirecting the Sentry and Art. 27 questions to privacy@1Password.com. 28 October 2026: RFI-IRFOS replies point by point, withdraws the "Secret Key exchange" wording (conceded, no other finding depended on it, the H1 rating is revisited on 17 November), presses on server-side key restriction with five named abuse paths, and copies privacy@1Password.com as directed. 10 November 2026: 1Password's security team replies again, naming the MDM/compensating-control rationale for H1 (which this report records as a documented, closed design question) and restating that key access is server-side controlled without naming the controls; the same day RFI-IRFOS replies, traces the Firebase Cloud Messaging auto-init override across 8.12.42/8.12.44, and withdraws the earlier credit for the auto-init manifest flag. 15 November 2026: RFI-IRFOS sends a status message six days before publication, raising L1 to L3 and the FCM auto-init as new points and setting five open questions. 17 November 2026 (01:29 UTC): 1Password confirms question 1 as closed, repeats that access to the keys and the storage bucket is controlled server-side and not published, and writes that the remaining concerns were forwarded to internal departments. The same day at 10:02 UTC RFI-IRFOS answers, lowers H1 from High to Medium, and addresses questions 4 to 6 on Sentry and the EU representative to privacy@1Password.com. As of 21 November 2026, no message from 1Password has arrived after that of 17 November 2026, and the security team has answered every question routed to it, on the key and bucket questions only with the statement that the configuration is not published. The privacy team, named by 1Password itself as the correct recipient on 27 October, has not replied to any of the three questions addressed to it in the twenty-four days since it was copied on 28 October 2026.

## What 1Password Got Right

- Biometric unlock via platform-native, hardware-backed APIs: AndroidX BiometricPrompt bound to a CryptoObject/AndroidKeyStore signing key, StrongBox hardware backing where available, and setInvalidatedByBiometricEnrollment, closing the attacker-enrolls-their-own-fingerprint bypass.
- Backup fully neutralized: both data_extraction_rules.xml and full_backup_content_rules.xml exclude all local app data domains, so no vault cache leaves the device via Android Backup or device-to-device transfer.
- Clean SDK inventory: no ad-tech, no attribution/analytics SDK beyond Sentry and Firebase (FCM only), and no sanctioned-jurisdiction SDK anywhere across all four dex files.
- A real per-event crash-report consent dialog (Send/Don't Send/Always Send), not silent automatic telemetry.
- A substantive, written engagement from the security team once the notice reached the right inbox, including a concession on RFI-IRFOS's own wording error and a documented design rationale for H1.
- Withdrawn in this report, per the correspondence of 10 November 2026: the original notice's credit for firebase_messaging_auto_init_enabled="false" as a genuine opt-in control. The manifest flag is overridden in code at every cold start when Google Play Services is available.

## Residual Risk & Recommendations

Closed by correspondence: H1's underlying design question (user-installed CA trust is deliberate, with named compensating controls). Open and unanswered by 1Password's named Privacy team as of 21 November 2026: M1 (Sentry pre-consent collection scope) and M3 (EU Art. 27 representative). Open and disputed, with 1Password's position recorded in full: M2 (server-side key restriction asserted but not named, and the newly discovered Firebase Cloud Messaging auto-init override). RFI-IRFOS continues weekly APK diffing against the archived 8.12.33, 8.12.42 and 8.12.44 builds through publication; any change to the network security configuration, the two keys, or the FCM auto-init call will be recorded against the correspondence record above, not treated as a reset of the embargo.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Root level code analysis of the published Google

Play release binary plus the operator's own public documentation and written correspondence. No 1Password servers, accounts, or backend keys were probed or tested. Research conducted under ISO/IEC 29147 and the freedom of scientific research (Art. 17 StGG). REF 1PASSWORD-2026-R1.