Coordinated Security & Privacy Disclosure, Final Report

Hallow for Android (app.hallow.android)

Seven written notices, ninety days, two broken escalation promises, zero substantive answers

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FIVE FINDINGS UNADDRESSED, ESCALATION PROMISED TWICE, NEVER DELIVERED

Target	Hallow
Product audited	Hallow for Android, app.hallow.android
Disclosure reference	REF HALLOW-2026-R1
R1 sent	2026-06-22
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2 a Huawei HMS advertising SDK collecting an advertising identifier from Catholic prayer-session behavior and routing it to PRC infrastructure, CVSS v4.0 8.7, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 22 June 2026, RFI-IRFOS performed static analysis of the production Hallow Android application, a Catholic prayer and meditation app, and identified two CRITICAL and three HIGH findings: a Firebase API key hardcoded in the shipped APK, a Huawei HMS advertising SDK that collects the Huawei OAID advertising identifier from EU users' prayer-session behavior and routes it to Huawei Technologies Co., Ltd. in the PRC, subject to China's National Security Law Art. 7, with no EU adequacy decision for China and no disclosure of this specific processing in the privacy policy, a Branch.io deep-link attribution SDK performing device fingerprinting linked to prayer-app behavior with no disclosed Art. 46 standard contractual clauses for this US-bound transfer, a Network Security Configuration containing only debug overrides and no production certificate pinning, and RECORD_AUDIO and READ_CONTACTS permissions requested with no functional justification identified for the contacts permission and no disclosure of audio recording during religious practice sessions.

Across seven written notices over ninety days, every substantive reply in this case came from Hallow's general support queue rather than a data-protection or privacy function. On 18 August, a support agent sent a genuinely attentive reply that named each technical finding by category, Firebase credentials, Huawei Mobile Services, Branch.io, certificate pinning, and permissions, and explicitly promised escalation to the appropriate internal team for a direct written response. No team member ever followed up with that response, and no reply of any kind, before or after that promise, answered any of RFI-IRFOS's three standing questions: whether the Huawei HMS routing of religious-behavior data to China is disclosed anywhere in the privacy policy, whether the hardcoded Firebase key has been rotated, and whether this would be addressed before or after a regulator made direct contact.

Scope: Static analysis of the publicly downloaded production Hallow Android APK, on an authorized test device, only. No Hallow account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 22 June 2026 to privacy@hallow.app. Across seven written notices over ninety days, every substantive reply came from the general support queue rather than a data-protection or privacy function; one support reply on 18 August explicitly named the technical findings and promised escalation to the appropriate team, but no team member ever answered any of the three standing questions, and a second escalation implied by the pattern of automated queue acknowledgments similarly produced nothing.

ID	Severity	Title
C1	CRITICAL	Firebase API key hardcoded in the production APK
C2	CRITICAL	Huawei HMS advertising SDK collects an advertising identifier from prayer-session behavior, routed to the PRC
H1	HIGH	Branch.io deep-link attribution – undisclosed device fingerprinting

ID	Severity	Title
H2	HIGH	No certificate pinning – only debug overrides in the Network Security Config
H3	HIGH	RECORD_AUDIO and READ_CONTACTS permissions unjustified

Subject & Operator Analysis

Hallow is a Catholic prayer and meditation application. Its published contacts for privacy and support matters are privacy@hallow.app and support@hallow.app respectively.

Findings

C1: Firebase API key hardcoded in the production APK

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

A Firebase API key is hardcoded in res/values/strings.xml of the production binary.

Whether this key has been rotated since disclosure was one of three standing questions never answered.

Impact: A production Firebase project's attack surface cannot be independently ruled safe from outside the console once its key ships in every installed client.

Fix: Rotate the exposed key, confirm deny-by-default security rules, and enforce App Check for this project.

C2: Huawei HMS advertising SDK collects an advertising identifier from prayer-session behavior, routed to the PRC

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

The Huawei HMS advertising SDK collects the Huawei OAID advertising identifier from EU users' Catholic prayer sessions (code reference n50/b.smali, 'Caught getHuaweiAdvertisingInfoObject exception:'), with data routed to Huawei Technologies Co., Ltd. in the PRC, subject to China's National Security Law Art. 7. No EU adequacy decision exists for this transfer, and it is not disclosed in the privacy policy.

Whether this routing is disclosed anywhere in the privacy policy was one of three standing questions never answered.

Impact: Data reflecting religious practice, a special category under GDPR Art. 9, may be transmitted to a PRC-jurisdiction recipient with no disclosed transfer mechanism.

Fix: Remove or geographically restrict the Huawei HMS advertising integration for EU users, or disclose the transfer explicitly with a valid Art. 44-49 mechanism.

H1: Branch.io deep-link attribution – undisclosed device fingerprinting

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

Branch.io (a US company) performs device fingerprinting linked to prayer-app behavior. Standard contractual clauses would be required for this transfer but are not disclosed.

No reply of any kind addressed this finding.

Impact: Device fingerprints linked to prayer-app usage behavior may be transferred to a US processor with no disclosed transfer mechanism.

Fix: Disclose Branch.io explicitly as a processor with the applicable Art. 46 transfer mechanism.

H2: No certificate pinning – only debug overrides in the Network Security Config

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 Configuration contains only debug overrides; no production certificate pinning exists for any endpoint.

No reply of any kind addressed this finding.

Impact: Traffic carrying religious-practice and personal data can be intercepted or altered by any party able to install a trusted certificate on the network path.

Fix: Implement certificate pinning for all production endpoints.

H3: RECORD_AUDIO and READ_CONTACTS permissions unjustified

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

RECORD_AUDIO and READ_CONTACTS are both requested on a prayer app. No functional justification for READ_CONTACTS was identified, and audio recording during religious practice sessions is not disclosed.

No reply of any kind addressed this finding.

Impact: Audio from religious practice sessions and a user's contact list may be accessible with no disclosed purpose for either.

Fix: Remove READ_CONTACTS if unused, and disclose any RECORD_AUDIO use explicitly, including its retention and purpose.

An Attentive Support Reply, an Escalation That Never Arrived

On 18 August, a Hallow support agent sent a reply that stood out among this case's otherwise automated queue acknowledgments: it named each technical finding by category and explicitly acknowledged that the disclosure required 'a substantive reply from the right team, not a support queue response,' promising escalation. No team member ever sent that follow-up. Every other reply in the case, before and after that message, was an identical automated queue-assignment acknowledgment. No reply of any kind, from privacy@hallow.app or any escalated function, ever answered RFI-IRFOS's three standing questions.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32	Hardcoded Firebase key
C2	GDPR Art. 9(1), Art. 13(1)(e), Art. 44	Undisclosed PRC-jurisdiction transfer of religious-practice-linked advertising data
H1	GDPR Art. 13(1)(e), Art. 46	Undisclosed US device-fingerprinting transfer
H2	GDPR Art. 32(1)(a)	No production certificate pinning
H3	GDPR Art. 5(1)(c), Art. 13	Unjustified contacts permission, undisclosed audio recording

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-22	R1 sent to privacy@hallow.app; 2 CRITICAL + 3 HIGH findings; remediation tiers of EUR 4,500/9,000/18,000 referenced under the R1 policy then in force – historical record only, not a currently open offer
2026-07-17	Follow-up, twenty-five days silence, Austrian DSB and EDPS added to cc, three questions posed
2026-08-18	Support agent replies, names the findings by category, promises escalation to the appropriate team; no follow-up ever arrives
2026-09-01	Follow-up adds the Irish DPC to cc
2026-09-12	Follow-up, eighty-two days, 'escalation promised twice, still no substantive reply'
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Follow through on the escalation to a data-protection function that was explicitly promised on 18 August.
- Remove or geographically restrict the Huawei HMS advertising integration for EU users.
- Disclose Branch.io explicitly as a processor with the applicable Art. 46 transfer mechanism.
- Implement certificate pinning for all production endpoints.
- Remove READ_CONTACTS if unused, and disclose any RECORD_AUDIO use explicitly.

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. GDPR Art. 5, 9, 13, 32, 44, 46. REF HALLOW-2026-R1.