Coordinated Security & Privacy Disclosure, Final Report

SAP Android Ecosystem (5 apps)

Field Service Management, JAM, Asset Manager, Mobile Start, SuccessFactors, eleven tickets, most substantive engagement of the research series, most still disputed

PUBLIC DISCLOSURE, PUBLISHED 24 SEPTEMBER 2026, THREE DAYS AFTER THE 21 SEPTEMBER EMBARGO – NINETY-FIVE DAYS, ELEVEN TICKETS, SIX WEEKS AND THREE CLOSURE RATIONALES, ONE QUESTION NEVER ANSWERED

Target	SAP SE, Walldorf, Germany
Products audited	SAP Field Service Management (com.sap.fsm), SAP JAM (com.sap.jam.android), SAP Asset Manager (com.sap.mobile.apps.assetmanager.release), SAP Mobile Start (com.sap.mobile.apps.sapstart), SAP SuccessFactors (com.successfactors.successfactors)
Disclosure reference	REF SAP-ANDROID-2026-R1, tickets PSINC0012180/0012183-0012187/0012190-0012194
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-21
Report published	2026-09-24, three days after the 2026-09-21 embargo, an internal publishing gap, not a change in terms
Severity	CRITICAL (C2, hardcoded Firebase keys x5, CVSS v4.0 9.3)

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 five SAP Android applications and identified eleven findings across two CRITICAL and four MEDIUM class, one of the MEDIUM-band findings (C1) held at CRITICAL under an explicit blast-radius escalation, spanning eleven individually ticketed items. The most significant: a Baidu Push SDK, 315 smali classes, is compiled into SAP Field Service Management, an app used by field engineers with access to industrial and critical-infrastructure client sites, alongside ACCESS_BACKGROUND_LOCATION and ACTIVITY_RECOGNITION permissions. Baidu is a PRC entity subject to China's National Intelligence Law (2017).

Separately, hardcoded Firebase API keys were extracted verbatim from all five applications' production binaries. On 29 July 2026, RFI-IRFOS specified fifteen individually reproducible abuse paths for this credential class: quota exhaustion, FCM token enumeration, Firestore unauthenticated read/write, storage bucket exposure, password-reset flooding, test-user creation flooding, Remote Config manipulation, Cloud Functions invocation, Crashlytics data injection, Dynamic Links abuse, App Check bypass, crash-reporting impersonation, Maps-quota drain, and project enumeration/IAM probing. None of the fifteen was individually addressed at any point in the correspondence.

SAP's Product Security Response Team engaged more substantively and more quickly than any other target in this year's audit series, assigning individual ticket numbers within five days and, on 6 August, producing a fully itemized classification of all eleven tickets. Two of eleven items (H3, M1) were substantively conceded, an unused permission scheduled for removal and an accepted risk tied to a planned app retirement. The remaining nine, including both CRITICAL findings, were classified No Security Vulnerability, Informational, By Design, or False Positive, without a technical rebuttal of the fifteen named abuse paths. A final message on 9 September stated the matter was 'resolved and closed' in full, without naming a single finding. All eleven findings stand exactly as originally reported, with SAP's own classification recorded alongside each.

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

Disposition

R1 sent 21 June 2026 to security@sap.com, cc privacy@sap.com. SAP's Product Security Response Team (PSRT) assigned individual ticket numbers to all eleven findings within five days, the most structured intake response of the research series. What followed was six weeks of shifting closure rationales: a retainer-proposal mischaracterization on 15 July, an unqualified assessment-complete closure on 28 July naming no finding, and a fully itemized per-ticket classification table on 6 August that engaged with content for the first time. A generic 'resolved and closed' reply on 9 September, and RFI-IRFOS's specific question about fifteen named abuse paths for the hardcoded Firebase keys, remained unanswered through the close of the embargo.

ID	Severity	Title
C1	CRITICAL	Baidu Push SDK compiled into SAP Field Service Management, a PRC entity on devices with background location access
C2	CRITICAL	Hardcoded Firebase API keys extracted verbatim from all five audited applications
H1	MEDIUM	Dynatrace OneAgent SDK, undisclosed Art. 28 processor, two apps
H2	MEDIUM	SYSTEM_ALERT_WINDOW, RECORD_AUDIO, WRITE_CONTACTS in SAP SuccessFactors, an HR application
H3	MEDIUM	AD_ID and READ_PHONE_STATE in a B2B-only field-service application
M1	MEDIUM	No network security configuration in SAP JAM

Subject & Operator Analysis

SAP SE (Walldorf, Germany) operates a portfolio of enterprise applications used across field service, collaboration, asset management, and human resources functions, deployed to employee and field-engineer devices, not consumer accounts.

Positive Observations

- SAP SuccessFactors' network security configuration pins over 100 production domains with explicit SAP CA roots, the most thorough certificate pinning found across five apps in this bundle.
- SAP Asset Manager enforces cleartextTrafficPermitted="false" with a custom DigiCert root.
- All five applications set android:allowBackup="false".
- SAP's Product Security Response Team assigned individual ticket numbers to all eleven findings within five days of the original disclosure, the fastest structured intake response of the research series.
- Two of eleven tickets (H3, M1) received specific, named, reasoned closures RFI-IRFOS does not dispute; one further ticket (H2) received specific per-permission feature justifications RFI-IRFOS records as noted.

Findings

C1: Baidu Push SDK compiled into SAP Field Service Management, a PRC entity on devices with background location access

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

315 Baidu smali classes are compiled into com.sap.fsm, including a signature-level push-info-provider permission and a dedicated device-identifier collection class, co-existing in the same app with ACCESS_BACKGROUND_LOCATION and ACTIVITY_RECOGNITION. RFI-IRFOS blast-radius escalation: raised from HIGH/8.7 to CRITICAL because the affected devices belong to field engineers with physical access to power grids, water systems, and industrial plants, a critical-infrastructure population CVSS's technical vector does not capture.

```
<permission android:name="baidu.push.permission.WRITE_PUSHINFOPROVIDER.com.sap.fsm"
    android:protectionLevel="signature"/>

com/baidu/pushservice/PushService.smali
com/baidu/push/cid/DeviceId.smali          <- device-identifier collection
com/baidu/android/pushservice/BasicPushNotificationBuilder.smali
com/baidu/push/cid/Util.smali
+ 311 further Baidu classes
```

SAP PSRT's ticket classification (PSINC0012180): No Security Vulnerability. Stated rationale, verbatim: "Accounts hosted in China use Baidu Push, while accounts hosted outside China use Firebase Cloud Messaging. No personal user data is collected or transmitted through the push notification service." This does not address the finding raised: SAP Field Service Management is a single global binary distributed to all EU users through the Google Play Store, not a China-region build. RFI-IRFOS's static analysis confirms the Baidu SDK is compiled into that global binary regardless of the account's hosting region, and a compiled SDK with a functioning device-identifier class present in an installed application is capable of executing independent of which push channel a given account happens to route through at runtime. SAP has not disputed that the SDK is present in the EU-distributed binary, only that it asserts the SDK does not activate for non-China accounts, a runtime claim RFI-IRFOS's static analysis cannot itself confirm or refute, and one SAP has not supported with a technical explanation of the gating mechanism.

Impact: A field engineer's device with access to industrial and critical-infrastructure client sites carries compiled code from a PRC push-notification vendor subject to the National Intelligence Law (2017), with a functioning device-identifier collection class present in the binary regardless of runtime account region.

Fix: Remove the Baidu SDK from the globally-distributed EU binary entirely, or publish the specific runtime gating mechanism and its verification method, and register Baidu as a named Art. 28 sub-processor with a Chapter V transfer safeguard if it is not fully inert outside China.

C2: Hardcoded Firebase API keys extracted verbatim from all five audited applications

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3

A distinct, valid Firebase API key was extracted from res/values/strings.xml in each of the five audited applications.

```
SAP Field Service Management (coresuite-9b45b):
  google_api_key:  AIzaSyAYUcQBKewpn6d3VyEpjKTVU4SkiwFEeEg
  google_maps_key: AIzaSyBC2m936z_o_Sa2oIJYfPsujMUXYPRsjNc
SAP JAM (sapjam-965):                 AIzaSyAB_4Egdlql9dq3FAkkmmMAae_rvhlu6O4
SAP Asset Manager (sap-asset-manager-b5e09): AIzaSyDeSspXmWCvnwA3mx_CX3oVWL0z0fl5ryo
SAP Mobile Start (sap-mobile-start):    AIzaSyCrD7aVkFsh3MYR7gyU5o6_bnIhX0x6Hy4
SAP SuccessFactors (sap-sf-crashlogs):  AIzaSyDFK7BFGpoOIZbNG6ESl500II9z53Cao3s
```

Ticket	App	SAP classification	SAP's stated rationale
PSINC0012183	Field Service Management	Informational / By Design	"Firebase API keys are intentionally included... not authentication secrets... governed separately through authentication and authorization controls."
PSINC0012184	JAM	False Positive	"associated with a legacy implementation... not used by the current implementation."
PSINC0012185	Asset Manager	Informational / By Design	Same boilerplate as FSM.
PSINC0012186	Mobile Start	Informational / By Design	Same boilerplate as FSM.
PSINC0012187	SuccessFactors	Informational / By Design	Same boilerplate as FSM.

On 29 July 2026, in response to the "not an authentication secret" position, RFI-IRFOS named fifteen individually reproducible abuse paths tied specifically to a public, unrestricted Firebase project key: quota exhaustion (availability), FCM token enumeration, Firestore unauthenticated read, Firestore unauthenticated write, storage bucket exposure, password-reset flooding, test-user creation flooding, Remote Config manipulation, Cloud Functions invocation, Crashlytics data injection, Dynamic Links abuse, App Check bypass, crash-reporting impersonation, Maps-quota drain (specific to the FSM Maps key), and project enumeration/IAM probing. This list was restated in full on 6 August, 25 August, and 11 September. At no point

did SAP's replies name, dispute, or concede any one of the fifteen individually; the JAM ticket's "legacy, not used" classification is the only one that engages with a specific operational claim, and it was not accompanied by confirmation that the key has been rotated or revoked.

Impact: A publicly extractable, unrestricted Firebase project key across five production applications enables, at minimum, quota exhaustion and enumeration attacks against SAP's own Firebase infrastructure, with the specific exposure profile of each of the fifteen abuse paths dependent on each project's actual security rules, which RFI-IRFOS's static analysis cannot itself verify and SAP has not disclosed.

Fix: For each of the five projects, publish the current Firestore/Storage security rules, confirm whether App Check is enforced, and address each of the fifteen named abuse paths individually, not as a single 'not a secret' classification; rotate the JAM key specifically if it is genuinely a legacy artifact still compiled into a distributed binary.

H1: Dynatrace OneAgent SDK, undisclosed Art. 28 processor, two apps

---

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

860 Dynatrace smali classes in Asset Manager (PSINC0012190), 249 in Mobile Start (PSINC0012191), instrumenting HTTP requests, view hierarchies, crashes, and user interactions.

SAP PSRT's classification for both tickets: No Security Vulnerability. Stated rationale, verbatim: "no personal data is processed… monitoring sessions are not linked across application launches." This is a claim about Dynatrace's specific configuration in these two apps, offered without supporting evidence (a Dynatrace configuration export, session-linking settings, or a data-processing agreement excerpt). RFI-IRFOS's finding is limited to the SDK's undisclosed presence as a data processor on devices handling physical asset inventories, maintenance records, and facility data; that presence itself is not disputed by SAP.

Impact: An Art. 28 processor instrumenting enterprise field-operations data is present without disclosed configuration detail sufficient for an independent party to verify SAP's own no-personal-data claim.

Fix: Publish the Dynatrace data-processing agreement and the specific configuration flags disabling personal-data capture and cross-session linking, or disclose Dynatrace as a named processor in the applicable privacy documentation.

H2: SYSTEM_ALERT_WINDOW, RECORD_AUDIO, WRITE_CONTACTS in SAP SuccessFactors, an HR application

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

Three permissions declared in an HR application handling performance data, salary bands, org charts, and succession planning, Art. 9-adjacent workforce data.

SAP PSRT's classification (PSINC0012192): No Security Vulnerability, but for the first time with individually named justifications for each permission, verbatim: "RECORD_AUDIO supports an optional profile audio feature; WRITE_CONTACTS supports an optional 'Save to Contacts' feature; SYSTEM_ALERT_WINDOW is used to display security warnings for certificate validation issues." RFI-IRFOS records this as noted, no further dispute; this is the kind of specific, feature-mapped answer RFI-IRFOS asked for on the remaining nine tickets and did not receive.

Impact: No further residual risk assessed once the specific feature justification is on record; the finding's disclosure and data-minimization documentation gap remains.

Fix: Document each permission's named feature and its optional status in the app's own privacy notice, so the justification SAP gave RFI-IRFOS is also visible to end users.

H3: AD_ID and READ_PHONE_STATE in a B2B-only field-service application

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

Advertising identifier and phone-state permissions declared in SAP Field Service Management, a B2B enterprise application with no consumer advertising use case.

SAP PSRT's classification (PSINC0012193): No Security Vulnerability. Stated rationale, verbatim: "currently unused… scheduled for removal as part of ongoing permission minimization efforts." RFI-IRFOS records this as conceded, and requests confirmation once the removal ships in a released build.

Impact: Minimal, given SAP's confirmation the permissions are unused; residual risk exists only until the scheduled removal ships.

Fix: Ship the scheduled removal and confirm the release version in which it lands.

M1: No network security configuration in SAP JAM

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

SAP JAM ships with no network security config file at all, affecting calendar sync and account authentication traffic.

SAP PSRT's classification (PSINC0012194): By Design / Accepted Risk. Stated rationale, verbatim: "protects data in transit using TLS and the Android system trust store... Given the application's planned retirement, the residual risk has been reviewed and accepted." RFI-IRFOS records this as a documented, reasoned risk acceptance, the only one of eleven tickets to explicitly name and accept residual risk, it does not dispute the finding's existence.

Impact: Limited, given SAP's documented and reasoned risk acceptance tied to a stated retirement plan for the application.

Fix: None required beyond SAP's own documented acceptance; RFI-IRFOS notes the app's continued availability on Google Play should be monitored against the stated retirement timeline.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 28, Chapter V; NIS2	PRC push SDK compiled into globally-distributed critical-infrastructure-adjacent app
C2	GDPR Art. 32, Art. 5(2)	Hardcoded, publicly extractable credentials across five apps, fifteen unaddressed abuse paths
H1	GDPR Art. 28	Undisclosed APM processor, two apps
H2	GDPR Art. 5(1)(c)	Permissions in HR app, feature justification now on record
H3	GDPR Art. 5(1)(c)	Unused permissions, removal scheduled
M1	GDPR Art. 32(1)(a)	No network security config, documented risk acceptance

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to security@sap.com, cc privacy@sap.com, 11 findings across 5 apps
2026-06-26	SAP (”Lorenzo”, PSRT) confirms receipt, assigns all 11 tickets individually within 5 days
2026-07-01	RFI-IRFOS separately notifies CERT-Bund/BSI on the C1 critical-infrastructure angle, ref #SAP-BSI-2026-001
2026-07-15	SAP (”Chisom”) closes case citing a retainer proposal RFI-IRFOS never made
2026-07-24 / 07-28	RFI-IRFOS corrects the retainer mischaracterization; SAP re-closes on different grounds, ”our assessment is complete”, naming zero findings
2026-07-29	RFI-IRFOS specifies fifteen individually reproducible abuse paths for the Firebase key finding
2026-08-06	SAP produces its fullest reply: itemized per-ticket classification table, first substantive engagement with individual findings; H3 and M1 conceded, H2 specifically justified, C1/C2/H1 disputed as unproven
2026-08-25 / 09-06 / 09-11	RFI-IRFOS restates the fifteen abuse paths and the five still-disputed findings by name; none individually addressed
2026-09-09	SAP (”PSRT”): ”SAP considers this matter resolved and closed on its side, with no further action required”, full text, naming zero findings
2026-09-21	Embargo, as stated identically throughout the correspondence, closes and this report publishes

SAP’s Product Security Response Team engaged more quickly and more specifically than any other target in this year’s audit series, and two of eleven tickets carry a reasoned, documented closure RFI-IRFOS does not dispute. The remaining nine tickets, including both CRITICAL findings, were closed with either boilerplate rationale unsupported by configuration evidence, or, in the final message, no named rationale at all. The specific, repeatedly restated question of which of fifteen named Firebase-key abuse paths SAP disputes and

which it accepts was never answered.

Residual Risk & Recommendations

- Publish the runtime gating mechanism preventing the Baidu Push SDK from activating on non-China SAP FSM accounts, or remove the SDK from the globally-distributed binary.
- Address each of the fifteen named Firebase-key abuse paths individually, with the actual security-rules configuration for each of the five Firebase projects.
- Publish the Dynatrace data-processing agreement and configuration detail supporting the no-personal-data claim for Asset Manager and Mobile Start.
- Ship the scheduled AD_ID/READ_PHONE_STATE removal from SAP Field Service Management and confirm the release version.
- Monitor SAP JAM's continued Play Store availability against the stated retirement timeline underlying its accepted network-security-config risk.

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 CVSS v4.0 is RFI-IRFOS's scoring guideline, not a ceiling or a floor. It gives a reproducible, third-party-legible starting point for severity, and it does not capture real-world blast radius on its own, factors such as user population size, a vulnerable or protected class of users, or a standing corporate governance exposure the technical vector alone cannot express. RFI-IRFOS reserves the right to weigh that blast radius above the bare CVSS score, and, more rarely, to hold a score below what CVSS alone would suggest when the underlying claim is unconfirmed or disputed with evidence. Any such escalation is always stated explicitly in the finding itself, never left implicit, as C1 is escalated in this report. Coordinated disclosure per ISO/IEC 29147. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 5, 28, 32, 44-49; NIS2 Directive. REF SAP-ANDROID-2026-R1.