Coordinated Security & Privacy Disclosure, Final Report

Salesforce Authenticator, Salesforce Maps, and Salesforce Chatter for Android (seven-app ecosystem audit)

Three case-number auto-replies, a PVR-portal redirect, three yes/no questions, and no reply of any kind from a human at any point

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – THREE CRITICAL FINDINGS UNADDRESSED, NO HUMAN REPLY EVER RECEIVED

Target	Salesforce, Inc., San Francisco, California, United States
Products audited	Salesforce Authenticator, Salesforce Maps, Salesforce Chatter for Android (part of a seven-app ecosystem audit)
Disclosure reference	REF SALESFORCE-2026-R1
R1 sent	2026-06-21 (approximate, inferred from the first case-number auto-reply)
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	HIGH (C1, hardcoded key in the MFA authenticator app itself, CVSS v4.0 8.8, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

RFI-IRFOS performed static analysis of three named applications within a seven-app Salesforce Android ecosystem audit and identified at least three CRITICAL findings: a hardcoded production Firebase key inside Salesforce Authenticator, the multi-factor-authentication app protecting access to Sales Cloud, Service Cloud, and Marketing Cloud, with confirmed active FCM push-authentication infrastructure; Salesforce Maps combining background location tracking, activity recognition, and a hardcoded internal endpoint into continuous field-employee location tracking with an empty network security configuration and no documented Art. 6(1) legal basis; and Salesforce Chatter trusting user-installed certificate authorities app-wide, including for salesforce.com traffic itself, on a CRM holding sales pipeline and customer records for over 150,000 enterprise customers. A systemic user-CA-trust and cleartext-permitted configuration was referenced as spanning further apps in the audited ecosystem, though those apps are not individually named in retrievable correspondence.

The original disclosure contact could not itself be recovered from this mailbox despite triggering three separate Salesforce support case numbers between 21 June and 9 July 2026; only the resulting automated acknowledgments and two later follow-ups that restate the findings verbatim are retrievable. RFI-IRFOS's 24 August 2026 follow-up states that a Product Vulnerability Response portal interaction redirected it away from email-based disclosure; this report records that claim as RFI-IRFOS's own account of an exchange that occurred outside this correspondence, not as an independently verified Salesforce statement, since no such message exists in the searched mailbox.

On 4 September 2026, RFI-IRFOS restated all three findings in full technical detail and posed three direct questions: whether the Firebase key has been rotated, what Art. 6(1) legal basis exists for Salesforce Maps' background location tracking, and whether Salesforce has notified any supervisory authority under GDPR Art. 33. A response deadline of 11 September 2026 passed with no reply. No supervisory authority was cc'd on any message in this specific case, unlike the majority of RFI-IRFOS's parallel disclosure cases, and no human, security-team, or product-vulnerability-response message of any kind was ever received.

Scope: Static analysis of publicly downloaded production Salesforce Android APKs (Authenticator, Maps, Chatter), on an authorized test device, only. No Salesforce account, backend, or infrastructure was accessed or tested.

Disposition

RFI-IRFOS's original disclosure contact triggered three separate Salesforce support case numbers between 21 June and 9 July 2026, each acknowledged only by an identical automated template. RFI-IRFOS's own 24 August 2026 follow-up states that a Product Vulnerability Response portal case told it security@salesforce.com no longer accepts disclosures by email; that exchange occurred, if at all, outside this correspondence and is recorded here as RFI-IRFOS's own account, not as a verified Salesforce statement. No human reply of any kind was ever received in this case.

ID	Severity	Title
C1	CRITICAL	Hardcoded production Firebase key inside Salesforce Authenticator, the MFA app itself
C2	CRITICAL	Salesforce Maps: continuous background location tracking, no documented legal basis
C3	CRITICAL	Salesforce Chatter trusts user-installed certificate authorities app-wide, including for salesforce.com traffic

Subject & Operator Analysis

Salesforce, Inc. is headquartered in San Francisco, California. No supervisory authority was cc'd on any message in this specific case, unlike the majority of RFI-IRFOS's parallel disclosure cases; this is recorded as an honest operational gap in this case's own handling, not attributed to Salesforce.

Findings

C1: Hardcoded production Firebase key inside Salesforce Authenticator, the MFA app itself

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N, 8.8

Firebase key AIzaSyB50xM40klFRoiK6h1REPceXsy4KrNQeks hardcoded inside Salesforce Authenticator, the multi-factor-authentication app protecting access to Sales Cloud, Service Cloud, and Marketing Cloud. FCM push authentication is confirmed active, meaning the production key for the push-MFA-challenge infrastructure ships in every downloaded APK.

RFI-IRFOS asked directly on 4 September 2026 whether this key has been rotated. No reply of any kind was received.

Impact: A hardcoded key inside the infrastructure responsible for delivering MFA push challenges raises the risk of forged or manipulated authentication prompts, in the application specifically trusted to secure access to Salesforce's own core products.

Fix: Rotate the key, restrict it to the app's package name and signing fingerprint, and publish confirmation that the MFA push-challenge flow cannot be forged using it.

C2: Salesforce Maps: continuous background location tracking, no documented legal basis

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

ACCESS_BACKGROUND_LOCATION, ACTIVITY_RECOGNITION, and a hardcoded internal endpoint (internal.na.sfmapsapi.com/liveapp/data/1) combine into continuous field-employee location tracking, with an empty network_security_config.

RFI-IRFOS asked directly on 4 September 2026 what Art. 6(1) legal basis governs this tracking. No reply of any kind was received.

Impact: Continuous location tracking of field employees operates with no demonstrated legal basis and no certificate pinning protecting the endpoint that receives it.

Fix: Publish the Art. 6(1) legal basis for this tracking, and implement certificate pinning on the internal endpoint.

C3: Salesforce Chatter trusts user-installed certificate authorities app-wide, including for salesforce.com traffic

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

Salesforce Chatter's network security configuration trusts user-installed certificate authorities app-wide, including for the primary salesforce.com traffic itself, on a CRM holding sales pipeline and customer records for over 150,000 enterprise customers.

Referenced in the 24 August 2026 follow-up as part of a systemic user-CA-trust and cleartext-permitted configuration spanning multiple apps in the audited ecosystem, though only Chatter is confirmed by name in retrievable correspondence. No reply of any kind was received.

Impact: Any actor with a system- or user-installed certificate can intercept and potentially manipulate traffic to and from Salesforce's own core CRM platform.

Fix: Remove user-CA trust from the network security configuration and pin Salesforce's own certificates.

A Redirect We Could Not Independently Verify

RFI-IRFOS's own 24 August 2026 follow-up states that a Salesforce Product Vulnerability Response portal case told it that security@salesforce.com no longer accepts disclosures by email. This report records that claim precisely as what it is: RFI-IRFOS's own account of an interaction that, if it occurred, took place outside the email correspondence examined for this report. No message containing that statement exists in the searched record, and it is not presented here as a verified Salesforce statement.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 32(2)	Hardcoded credential inside MFA-delivery infrastructure
C2	GDPR Art. 6(1), Art. 32(1)(a)	Undocumented legal basis for continuous employee location tracking
C3	GDPR Art. 32(1)(a)	App-wide user-CA trust on a CRM platform

Disclosure Timeline & Outcome

Date	Event
2026-06-21 through 07-09	Three separate case numbers generated (00279795, 00280128, 00282831), each acknowledged only by an identical automated template
2026-08-24	RFI-IRFOS declines a PVR-portal redirect as inapplicable to a statutory GDPR disclosure, restates C1 and C2, reaffirms the 19 September embargo
2026-09-04	RFI-IRFOS restates all three findings in full technical detail, poses three direct questions, sets an 11 September deadline
2026-09-11	Deadline passes with no reply
2026-09-19	Embargo, as stated identically in both retrievable follow-ups, closes and this report publishes

Residual Risk & Recommendations

- Rotate the Firebase key inside Salesforce Authenticator and confirm the MFA push-challenge flow cannot be forged using it.
- Publish the Art. 6(1) legal basis for Salesforce Maps' continuous background location tracking.
- Remove app-wide user-CA trust from Salesforce Chatter and pin Salesforce's own certificates.

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. Research activity protected under Austria's Forschungsfreiheitsgesetz (Art. 17 StGG). GDPR Art. 6, 32, 33. REF SALESFORCE-2026-R1.