Coordinated Privacy Disclosure, Final Report

Pinterest for Android (com.pinterest)

Pinterest, Inc. (NYSE: PINS), San Francisco, California, USA

SILENT ON SUBSTANCE · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, 91 DAYS AFTER DISCLOSURE, EIGHT MESSAGES, EIGHT IDENTICAL PRESS-BOT REPLIES, ZERO WORDS FROM SECURITY OR PRIVACY

Target	Pinterest for Android, v14.24.0 at the time of disclosure
Package	com.pinterest
Operator	Pinterest, Inc. (NYSE: PINS), San Francisco, California, USA
Initial Disclosure	2026-06-26
Original Embargo	2026-09-24 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, one day after the embargo, an internal publishing gap, not a change in terms
Regulators	Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz
Total Outbound Messages	8, across 91 days, to security@pinterest.com and privacy@pinterest.com, cc press@pinterest.com and legal@pinterest.com
Inbound Replies	8, every single one the identical automated out-of-office from press+noreply@pinterest.com. Zero replies, automated or human, from security@pinterest.com, privacy@pinterest.com, or legal@pinterest.com at any point.

rfi.irfos@gmail.com • rfi-irfos.com
ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

Executive Summary

On 26 June 2026, RFI-IRFOS disclosed six findings to Pinterest, Inc. concerning its Android application. Two of those findings carry full technical documentation recovered for this closing report: the app's network security configuration permits cleartext traffic globally, protecting only seven named domains in its base configuration while every other endpoint, including an undisclosed third-party SDK's own traffic, remains open to interception; and an undisclosed LINE Corporation SDK, 42 smali classes, routes authentication data to Japan and South Korea without appearing in Pinterest Europe Ltd's published processor list as verified at the time of disclosure.

Eight messages were sent to security@pinterest.com and privacy@pinterest.com, cc'ing press@pinterest.com and legal@pinterest.com, across 91 days. Every single one of the eight drew the identical automated out-of-office from press+noreply@pinterest.com, the same acknowledgment intended for press inquiries, not security or privacy correspondence. At no point across eight rounds and 91 days did security@pinterest.com, privacy@pinterest.com, or legal@pinterest.com send a single word back, not a substantive answer and not so much as an automated receipt. On a NYSE-listed platform of this size, a security and privacy inbox producing zero words across eight direct attempts is itself part of the record.

The 90-day embargo, set at first contact, elapsed on 24 September 2026. This report and the accompanying closure notice publish one day later, an internal gap on RFI-IRFOS's side, not a change to the terms already disclosed.

Scope: Root-level static analysis of the production Pinterest Android application (com.pinterest, v14.24.0), covering the network security configuration and decompiled dex/smali, as pulled and reviewed on 26 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Pinterest's backend infrastructure was performed. The original disclosure named six findings; this report restates the two for which full supporting technical evidence was recovered for this closing pass. The remaining four are not restated here, not because they were withdrawn, but because RFI-IRFOS does not publish a finding it cannot currently substantiate with the same evidentiary standard applied throughout this report.

Disposition

Six findings were disclosed on 26 June 2026. Two are detailed here with full technical evidence recovered for this closing report and re-scored under CVSS v4.0: global cleartext traffic permitted across the production application, with the network security configuration's base config protecting only seven named domains while every other endpoint remains open to interception, reaches HIGH on the computed CVSS score alone. An undisclosed LINE Corporation SDK, 42 smali classes routing authentication data to Japan and South Korea, absent from Pinterest Europe Ltd's published list of processors and sub-processors as verified at the time of disclosure, scores MEDIUM. The remaining four findings referenced across this correspondence are not restated in this closing report because their original supporting evidence could not be located for this pass, and RFI-IRFOS does not publish a finding it cannot currently substantiate. Eight messages were sent across 91 days. Every one drew the identical automated press-team acknowledgment. Not one word was ever received from security, privacy, or legal.

ID	Severity	Title
C1	HIGH	Global Cleartext Traffic Permitted, Seven Domains Protected, Everything Else Open to Interception
H1	MEDIUM	Undisclosed LINE Corporation SDK Routes Authentication Data to Japan and South Korea

Subject & Operator Analysis

Pinterest, Inc. (NYSE: PINS) operates the Pinterest visual discovery platform, with a global Android user base in the hundreds of millions. Six findings were disclosed on 26 June 2026; two are documented here with full recovered technical evidence.

Eight Rounds, Eight Identical Press Replies, Zero Words From Security or Privacy

This case's correspondence pattern is unusually clean within this campaign: a single automated reply, repeated verbatim on cue eight separate times, from an address, press+noreply@pinterest.com, that exists to acknowledge media inquiries, not GDPR disclosures. security@pinterest.com and privacy@pinterest.com, the two addresses this disclosure was actually sent to, along with legal@pinterest.com in cc throughout, never sent a single word back across 91 days, not a substantive answer and not so much as an automated receipt. On a platform of Pinterest's scale, a security and privacy inbox producing zero words across eight direct attempts is a data point in its own right.

Findings

C1: Global Cleartext Traffic Permitted, Seven Domains Protected, Everything Else Open to Interception

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. This finding reaches HIGH on the computed CVSS v4.0 score alone; no editorial escalation was applied or needed.

The network security configuration's base-config permits cleartext (unencrypted HTTP) traffic globally. Only seven named domains are individually configured to require HTTPS; every other endpoint the application communicates with, including traffic generated by the undisclosed LINE SDK (H1) and other bundled third-party libraries, falls back to the permissive cleartext default. A party positioned on the same network as a user, a shared WiFi network, a compromised router, an open access point, can intercept or manipulate this unprotected traffic.

Impact: Any user on a shared or compromised network is exposed to interception or manipulation of Pinterest application traffic that falls outside the seven explicitly protected domains, on a platform with a global user base in the hundreds of millions.

Fix: Set cleartextTrafficPermitted="false" in the network security configuration's base-config and enumerate exceptions individually if any are genuinely required, not default the entire application to permissive. No confirmation that this has occurred was ever received.

H1: Undisclosed LINE Corporation SDK Routes Authentication Data to Japan and South Korea

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

42 smali classes belonging to the LINE Corporation SDK are present in the production binary, routing authentication-related data to infrastructure in Japan and South Korea. As verified at the time of disclosure, LINE was absent from Pinterest Europe Ltd's published list of data processors and sub-processors.

```
LINE Corporation SDK: 42 smali classes confirmed in production binary
authentication-related data routed to endpoints in Japan and South Korea
not listed in Pinterest Europe Ltd's published processor/sub-processor list
(verified at time of disclosure, 2026-06-26)
```

Impact: Authentication-related data is routed to a named third-party processor in two jurisdictions outside the EEA, with no disclosed Art. 44-49 transfer mechanism and no entry in the published processor list at the time this was checked.

Fix: Name LINE Corporation individually as a data processor with a stated Art. 44-49 transfer mechanism in Pinterest's published processor documentation, or remove the dependency if not load-bearing. No confirmation that this has occurred was ever received.

Data Protection, Article by Article

The findings map onto a small, specific set of GDPR provisions, set out below in one place instead of scattered across the findings themselves.

Article	Finding	Basis
Art. 32(1)(b), Art. 25	C1	Global cleartext traffic exposes application data to interception on untrusted networks.
Art. 13(1)(e), Art. 44-49	H1	Undisclosed data processor routing authentication data outside the EEA.

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. In this report, C1 reaches HIGH on its computed CVSS v4.0 score alone. This report restates only the two findings, of the six originally disclosed, for which full technical evidence was recovered for this closing pass; the remaining four are not restated here because RFI-IRFOS does not publish a finding it cannot currently substantiate to the same evidentiary standard. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: PINTEREST-ANDROID-2026.