Coordinated Security & Privacy Disclosure, Final Report

TeamViewer for Android (com.teamviewer.teamviewer.market.mobile)

An acknowledgment, a blanket rejection naming zero findings, then "we consider this matter closed," followed by seventy-three days of total silence

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – FIVE FINDINGS, DECLARED CLOSED WITHOUT A SINGLE NAMED REBUTTAL

Target	TeamViewer SE / TeamViewer Germany GmbH, Göppingen, Germany
Product audited	TeamViewer for Android, com.teamviewer.teamviewer.market.mobile, v15.78.176
Disclosure reference	REF TEAMVIEWER-2026-R1
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C2, a proprietary update mechanism bypassing Google Play Store review on a remote-access tool, CVSS v4.0 9.2)

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

Contents

Executive Summary

On 20 June 2026, RFI-IRFOS performed static analysis of the production TeamViewer Android application and identified two CRITICAL and three HIGH findings: Sentry's session-replay module, active in production with 744 Sentry-related classes, capturing the app's own UI view hierarchy, corporate contact directories, connection history, active session metadata, and in-app technician chat, and transmitting it to Sentry Inc.'s US infrastructure, not named as a processor in TeamViewer's privacy documentation; a proprietary AppUpdateLib mechanism, paired with the MANAGE_EXTERNAL_STORAGE permission, that downloads and installs TeamViewer updates outside Google Play Store review, confirmed as a live dual-path installer rather than dormant code; the complete absence of a Network Security Config, meaning no TLS certificate pinning protects a remote-access tool's own infrastructure; undisclosed GPS-precision location access with no functional justification for a remote-support session; and Bluetooth MAC-address collection via all four Bluetooth permissions, also undisclosed.

TeamViewer Support replied three times in the first eighteen days. On 2 July 2026, a generic acknowledgment that the findings were under review. On 3 July 2026, a one-sentence rejection: "TeamViewer rejects the reported findings and does not classify them as security vulnerabilities or privacy issues," naming no finding individually. On 8 July 2026, a final statement: "At this stage, we do not intend to provide further technical commentary on the individual claims... We consider this matter closed," redirecting any further engagement to competent authorities.

No message of any kind, human or automated, arrived from TeamViewer after 8 July 2026, across five further written escalations and seventy-three days. RFI-IRFOS's final three questions, whether LfDI Baden-Württemberg ever received a direct technical response, whether an Art. 35 DPIA is on file for the Sentry session-replay integration, and whether Art. 33 supervisory notification occurred within 72 hours, were never answered.

Scope: Static analysis of the publicly downloaded production TeamViewer Android APK (v15.78.176), on an authorized test device, only. No TeamViewer account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 20 June 2026 to privacy@teamviewer.com, bcc the Austrian DSB, CERT.at, and LfDI Baden-Württemberg, TeamViewer's own lead supervisory authority. TeamViewer Support replied three times between 2 and 8 July 2026: an acknowledgment, a one-sentence blanket rejection naming zero findings individually, and a final statement declaring the matter closed and declining further technical commentary. No message of any kind, human or automated, has arrived since 8 July 2026, a silence of seventy-three days as of the embargo date.

ID	Severity	Title
C1	CRITICAL	Sentry Session Replay active on a remote-access platform, corporate session context transmitted to the US

ID	Severity	Title
C2	CRITICAL	Proprietary AppUpdateLib installer bypasses Google Play Store review
H1	HIGH	No Network Security Config, no certificate pinning on TeamViewer's own infrastructure
H2	HIGH	GPS-precision location access, no functional justification
H3	HIGH	All four Bluetooth permissions declared, MAC address collection confirmed

Subject & Operator Analysis

TeamViewer SE is headquartered in Göppingen, Baden-Württemberg, Germany, placing LfDI Baden-Württemberg as its lead supervisory authority, correctly identified and cc'd from the second notice onward in this case.

Findings

C1: Sentry Session Replay active on a remote-access platform, corporate session context transmitted to the US

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

744 Sentry-related classes, including a full RRWeb session-replay module, capture the app's own UI view hierarchy: corporate contact directories, IT-managed endpoint and device names, recent connection history, active session metadata, in-app technician-user chat, and authentication screens, and transmit it to Sentry Inc.'s San Francisco infrastructure.

Sentry is not named as a data processor in TeamViewer's privacy documentation. TeamViewer's 3 July reply rejected all findings as a category without naming this one individually; the 8 July reply declined to provide any further technical commentary.

Impact: Corporate remote-access session context, including which engineer connected to which infrastructure, is exposed to an undisclosed US third party.

Fix: Name Sentry explicitly as a processor, disable session replay of sensitive UI regions, and publish the applicable Art. 44-49 transfer mechanism.

C2: Proprietary AppUpdateLib installer bypasses Google Play Store review

CRITICAL, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N, 9.2

com.teamviewer.appupdatelib classes, paired with the MANAGE_EXTERNAL_STORAGE permission, download and install TeamViewer updates outside Play Store review. Apk InstallationSource$SwigNext explicitly tracks whether an update arrived via Play Store or the direct-install path, confirming a live, dual-path installer, not dormant code.

This bypasses Google Play Protect scanning and Play Store integrity verification on a remote-access tool used to reach banking, hospital, and corporate infrastructure, a supply-chain attack surface. TeamViewer's replies never addressed this finding by name.

Impact: A compromised update-delivery path could push a malicious update to TeamViewer installations without passing through Play Store's independent review.

Fix: Remove the direct-install update path and rely exclusively on Play Store-reviewed updates, or publish the integrity-verification mechanism that replaces Play Protect's review.

H1: No Network Security Config, no certificate pinning on TeamViewer's own infrastructure

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

No NSC file is present in the APK, and no TLS certificate pinning protects connections to teamviewer.com or the session relay servers.

For remote-access sessions transiting enterprise networks with deep packet inspection, or facing the possibility of rogue CA issuance, app-level pinning is the last line of defense. TeamViewer's replies never addressed this finding by name.

Impact: An actor with a system-trusted certificate can intercept remote-access session traffic.

Fix: Implement certificate pinning for teamviewer.com and all session relay endpoints.

H2: GPS-precision location access, no functional justification

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

Five smali files reference location APIs with GPS-precision access; no purpose is individually stated in TeamViewer's privacy documentation for a remote-desktop support tool.

TeamViewer's replies never addressed this finding by name.

Impact: Precise location data is collected with no stated functional need for a remote-support session.

Fix: Remove GPS-precision location access, or document the specific feature that requires it.

H3: All four Bluetooth permissions declared, MAC address collection confirmed

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

All four Bluetooth permissions are declared, and a confirmed BluetoothDevice.getAddress() call collects a persistent device identifier under GDPR.

No purpose is individually stated in TeamViewer's privacy documentation. TeamViewer's replies never addressed this finding by name.

Impact: A persistent hardware identifier is collected with no disclosed purpose.

Fix: Document the specific purpose for Bluetooth MAC collection, or remove it if unused.

Acknowledgment, Blanket Rejection, "This Matter Is Closed"

TeamViewer's three replies, in sequence, verbatim: "We are currently reviewing the reported information internally" (2 July); "TeamViewer rejects the reported findings and does not classify them as security vulnerabilities or privacy issues" (3 July, naming zero findings individually); "At this stage, we do not intend to provide further technical commentary on the individual claims... We consider this matter closed" (8 July). No reply of any kind followed across five further written escalations and seventy-three days.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 13(1)(e), Art. 44-49, Art. 32(1)(b)	Undisclosed US processor, corporate session data transferred
C2	GDPR Art. 25(1), Art. 32(1)(b)	Update mechanism bypassing independent store review
H1	GDPR Art. 32(1)(a)	No certificate pinning on remote-access infrastructure
H2/H3	GDPR Art. 5(1)(c), Art. 13(1)(c)	Undisclosed location and Bluetooth identifier collection

Disclosure Timeline & Outcome

Date	Event
2026-06-20	R1 sent to privacy@teamviewer.com, bcc Austrian DSB/CERT.at/LfDI Baden-Württemberg, 2 CRITICAL + 3 HIGH findings
2026-07-02	First reply: generic acknowledgment
2026-07-03	Second reply: blanket rejection naming zero findings individually
2026-07-08	Third and final reply: ”we consider this matter closed,” declines further technical commentary
2026-07-17 through 2026-08-15	Three escalations restate the findings and rebut the closure posture; no reply
2026-09-03 / 09-11	Final escalations pose three closing questions on LfDI BW contact, an Art. 35 DPIA, and Art. 33 notification; no reply
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Answer, on the technical merits, which finding is disputed and why, rather than a blanket rejection.
- Confirm whether LfDI Baden-Württemberg has received a direct technical response and whether an Art. 35 DPIA covers the Sentry integration.
- Remove the direct-install update path (C2) and rely on Play Store review.

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. 5, 13, 25, 32, 33, 35, 44-49. REF TEAMVIEWER-2026-R1.