Coordinated Privacy Disclosure, Final Report

Caritas Intranet Android (org.xinger.caritasintranet)

Caritas der Erzdiözese Wien, Albrechtskreithgasse 19-21, 1160 Wien, Austria

CEASE-AND-DESIST ATTEMPTED, FULLY REBUTTED, THEN SILENT · CASE CLOSED AND PUBLISHED 25 SEPTEMBER 2026, ON THE ORIGINAL EMBARGO DATE

Target	Caritas Intranet, an internal staff Android app for Caritas der Erzdiözese Wien employees (rosters, announcements, internal systems access)
Package	org.xinger.caritasintranet
Operator	Caritas der Erzdiözese Wien, Albrechtskreithgasse 19-21, 1160 Wien, Austria
Initial Disclosure	2026-06-27
Original Embargo	2026-09-25 (90 days from disclosure, as stated in the original notice)
Report Published	2026-09-25, on the original embargo date
Regulators	Austrian DSB, CERT.at
Total Outbound Messages	8, across 90 days: three technical messages (27 June, 30 June, 6 July) to datenschutz@caritas-wien.at and it@caritas-wien.at, one full technical and legal rebuttal (9 July) and three further follow-ups (15 July, 15 August, 25 August) to Caritas's external counsel.
Inbound Replies	1, a formal cease-and-desist letter from Jank Weiler Operenyi Rechtsanwälte GmbH (Deloitte Legal Austria), received 9 July 2026, asserting without technical detail that the reported findings did not exist and demanding retraction, a signed non-disparagement undertaking, and penalty payments. No technical rebuttal of any specific finding was ever received, before or after.

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 27 June 2026, RFI-IRFOS disclosed to Caritas der Erzdiözese Wien that its mandatory employee intranet app implements legacy LM and NTLM password hashing (createLMHashedPasswordV1, createNTHashedPasswordV1, createNTHashedPasswordV2, confirmed in compiled binary code), a protocol Windows itself has disabled by default since 2006 because it is crackable with a consumer graphics card in minutes via rainbow tables, contingent on whether the server still accepts LM negotiation. The same production APK hardcodes plaintext references to multiple internal Caritas server environments, production, test, and development, plus a direct link to an internal wiki, giving anyone who downloads the public app from the Play Store a map of internal systems within minutes. android:cleartextTrafficPermitted is set to true globally, meaning credentials could transit in plaintext over an open network in combination with the hashing weakness above.

Three technical messages across ten days drew no reply of any kind. On 9 July 2026, Caritas's external counsel, Jank Weiler Operenyi Rechtsanwälte GmbH, part of the Deloitte Legal network, sent a formal cease-and-desist letter. Its entire substantive content on the technical merits was one sentence stating the reported violations did not exist, with no counter-evidence, no citation, and no rebuttal of any individual finding. The letter simultaneously accused RFI-IRFOS of unfair competition and reputational harm, demanded permanent deletion of the public ledger entry, and required a signed undertaking carrying a EUR 2,000-per-day penalty payable directly to the law firm's own account, with personal liability extended to RFI-IRFOS's chairman, by a deadline five days later.

RFI-IRFOS replied the same day with a complete technical and legal rebuttal, addressing each of the five findings individually with its own code citation, declining to sign the undertaking, and rejecting the personal-liability theory. As a voluntary, good-faith coordinated-disclosure concession, independent of the letter's demands and independent of the findings' accuracy, RFI-IRFOS withheld the specific internal server addresses named in the original finding from further external communication and from this report, since responsible disclosure withholds exploitable specifics while a gap remains unconfirmed as fixed; the underlying finding that such addresses are exposed stands unchanged. Three further follow-ups, on 15 July, 15 August, and 25 August 2026, restated three yes/no technical questions and drew no response of any kind from counsel, Caritas, or the diocese. The 90-day embargo, set at first contact, elapses today, 25 September 2026, and this report publishes on that date.

Scope: Root-level static analysis of the production Caritas Intranet Android application (org.xinger.caritasintranet, version 1.5.1), as reviewed on 27 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Caritas's backend infrastructure was performed. Specific internal server addresses are withheld from this report as a voluntary coordinated-disclosure concession, independent of Caritas's own dispute of the findings.

Disposition

Five findings were disclosed on 27 June 2026, re-scored under CVSS v4.0. Legacy LM/NTLM hash authentication reaches CRITICAL on the computed CVSS score alone. Cleartext network traffic permitted by default also reaches HIGH on the computed score alone. Internal server environment exposure, an undisclosed US push-notification processor, and pre-consent Firebase initialization in a mandatory employee app all correct to MEDIUM. On 9 July 2026, twelve days after disclosure and after three unanswered technical messages, Caritas's external counsel sent a cease-and-desist letter asserting, in a single unsupported sentence, that the reported findings did not exist, while separately demanding retraction, a signed undertaking, and per-day penalty payments including personal liability. RFI-IRFOS replied the same day with a full technical and legal rebuttal, declined to sign, and voluntarily withheld the specific internal server addresses from public disclosure as a coordinated-disclosure concession, independent of their accuracy. Three further follow-ups drew no response of any kind.

ID	Severity	Title
C1	CRITICAL	Legacy LM/NTLM Hash Authentication Compiled Into the App
C2	HIGH	Cleartext Network Traffic Permitted by Default
H1	MEDIUM	Internal Server Environments and an Internal Wiki Link Exposed in the Public Production Binary
H2	MEDIUM	OneSignal, a US Push-Notification Processor, Used for Employee Communications Without a Documented Art. 46 Safeguard
H3	MEDIUM	Firebase Initializes Before Any Technical Possibility of Consent, in a Mandatory Employee App

A Cease-and-Desist Letter Containing One Unsupported Sentence on the Technical Merits

This case's correspondence record includes a formal legal response, not silence throughout. On 9 July 2026, twelve days after disclosure and after three unanswered technical messages, Jank Weiler Operenyi Rechtsanwälte GmbH, part of the Deloitte Legal network and, notably, also Caritas Wien's own external data protection counsel, sent a four-page cease-and-desist letter. Its entire substantive engagement with the technical findings was a single sentence stating the alleged violations did not exist, with no counter-evidence, no citation, and no individual rebuttal. The letter separately alleged unfair competition and reputational harm, demanded permanent deletion of the public ledger entry, and attached a undertaking requiring a EUR 2,000-per-day penalty payable to the law firm's own account, with liability extended personally to RFI-IRFOS's chairman, by a deadline five days later.

RFI-IRFOS replied the same day with a full technical and legal rebuttal addressing each finding individually, declined to sign the undertaking, and rejected the personal-liability theory, while accepting responsibility for the organization's own communications as its chairman. As a voluntary, good-faith concession consistent with ISO/IEC 29147 coordinated disclosure, and independent of the letter's demands, RFI-IRFOS withheld the specific internal server addresses from further external communication; the underlying finding that such addresses were exposed at the time of review stands unchanged. Three further follow-ups, on 15 July, 15 August, and 25 August 2026, restated three specific yes/no technical questions, whether legacy hash negotiation is still accepted, whether the internal environment addresses have been removed from the public build, and whether the Austrian DSB was notified under Art. 33, and drew no response of any kind from counsel, Caritas, or the diocese CC'd on later rounds.

Findings

C1: Legacy LM/NTLM Hash Authentication Compiled Into the App

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

createLMHashedPasswordV1, createNTHashedPasswordV1, and createNTHashedPasswordV2 are all confirmed present in the compiled binary (libapp.so). LM hashing has been disabled by default in Windows since Vista in 2006 specifically because it is crackable with a consumer graphics card in minutes via rainbow tables; whether it is actually exploitable in practice depends on whether the authenticating server still accepts LM negotiation, which RFI-IRFOS could not confirm without further engagement Caritas never provided.

```
createLMHashedPasswordV1 / createNTHashedPasswordV1 / createNTHashedPasswordV2 (
    confirmed in libapp.so)
```

Impact: If the authenticating server accepts LM negotiation, employee credentials for a mandatory work app are exposed to a well-understood, trivially automatable cracking technique that has been considered obsolete and insecure for nearly two decades.

Fix: Confirm and disable LM/NTLM negotiation on the authenticating server, and migrate to a modern authentication protocol. No confirmation that this has occurred was ever received.

C2: Cleartext Network Traffic Permitted by Default

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.

android:cleartextTrafficPermitted is set to true as a global base configuration, meaning unencrypted HTTP is permitted by default across the app, not scoped to any specific legacy endpoint.

```
cleartextTrafficPermitted="true" (global base configuration)
```

Impact: In combination with the legacy hashing finding above, credentials and internal data could transit in plaintext over an open or compromised network, such as public WiFi.

Fix: Set cleartextTrafficPermitted to false globally and configure per-domain exceptions only where strictly necessary. No confirmation that this has occurred was ever received.

H1: Internal Server Environments and an Internal Wiki Link Exposed in the Public Production Binary

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.

Multiple internal Caritas server environment hostnames, spanning production, test, and development, plus a direct link to an internal wiki, are hardcoded in plaintext in the publicly downloadable production APK. Specific hostnames are withheld from this report as a voluntary coordinated-disclosure concession; the underlying exposure, confirmed at the time of review, stands.

Impact: Anyone who downloads the public app from the Play Store can extract a map of internal systems, including test and development environment addresses, within minutes.

Fix: Remove all non-production environment hostnames and internal wiki links from the public production build, and route configuration through a mechanism that does not embed internal addresses in a publicly distributed binary. No confirmation that this has occurred was ever received.

H2: OneSignal, a US Push-Notification Processor, Used for Employee Communications Without a Documented Art. 46 Safeguard

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.

OneSignal, a US company, is used for internal employee push notifications, rosters, and announcements, across multiple Caritas units. No Art. 46 GDPR transfer safeguard documentation was located.

Impact: Employee scheduling and internal announcement data transits a US-based processor with no documented transfer safeguard, in a mandatory work application, an Art. 88 employee-data-protection consideration.

Fix: Document an Art. 46 transfer mechanism for OneSignal or migrate to an EU-based push provider. No confirmation that this has occurred was ever received.

H3: Firebase Initializes Before Any Technical Possibility of Consent, in a Mandatory Employee App

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.

FirebaseInitProvider is declared with initOrder=0 and directBootAware=true, meaning Firebase Analytics starts before any user interaction and before any technical mechanism for consent could run. Since this is a mandatory app employees are required to use for work, the consent question here is an Art. 88 employee-data-protection matter, not a standard consumer-consent one.

```
FirebaseInitProvider  initOrder=0, directBootAware=true
```

Impact: Analytics collection begins in a mandatory work app before any consent mechanism could technically exist, a distinct Art. 88 concern given employees cannot simply decline to use a required work tool.

Fix: Defer FirebaseInitProvider initialization and document the Art. 88 legal basis for any analytics collection in a mandatory employee app. 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	C1	Legacy, crackable password-hashing scheme compiled into a mandatory employee app.
Art. 32	C2	Cleartext network traffic permitted by default.
Art. 32, Art. 5(1)(f)	H1	Internal server environments and an internal wiki exposed in a public production binary.
Art. 46, Art. 88	H2	Undisclosed US push-notification processor for mandatory employee communications.
Art. 7, Art. 88	H3	Pre-consent analytics initialization in a mandatory work application.

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. In this report, C1 reaches CRITICAL and C2 reaches HIGH on their computed CVSS v4.0 scores alone, no editorial escalation applied; H1, H2, and H3 correct to MEDIUM to match their own computed bands. Specific internal server addresses named in the original 27 June 2026 disclosure are withheld from this public report as a voluntary coordinated-disclosure concession, independent of their accuracy or of Caritas's dispute of the findings. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF REF: CARITASWIEN-2026-R1.