Coordinated Security & Privacy Disclosure, Final Report

Opera Browser Android (com.opera.browser)

Opera Norway AS, publicly listed as Opera Limited (NASDAQ: OPRA)

ENGAGED · CASE CLOSED AND PUBLISHED 23 SEPTEMBER 2026, ON THE ORIGINAL EMBARGO DATE, THREE CORE QUESTIONS STILL NEVER ANSWERED

Target	Opera Browser for Android, a mainstream mobile browser with a very large global install base
Package	com.opera.browser, version 99.3.5094.89092 at time of disclosure
Operator	Opera Norway AS, headquartered in Oslo, Norway, part of the Opera group of companies publicly listed on NASDAQ as Opera Limited (OPRA)
Lead Supervisory Authority	Norwegian Datatilsynet
Initial Disclosure	2026-06-25
Original Embargo	2026-09-23 (90 days from disclosure)
Case Closed	2026-09-23, on the original embargo date
Regulators in BCC	Norwegian Datatilsynet, Austrian DSB, CERT.at
Correspondents	press-team, privacy inbox (automated only), and Michael Tegos, Product Marketing Manager, Privacy and Security, the only human respondent across the case
Total Outbound Messages	9, across 90 days

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

Contents

Executive Summary

On 25 June 2026, RFI-IRFOS disclosed to Opera that its Android browser compiles ByteDance's Pangle ad SDK as a first-class component, that Opera Software AS's shareholding at the time included two PRC-incorporated entities subject to China's National Intelligence Law Art. 7, that the ad system, including Pangle, auto-initializes via a ContentProvider before any consent screen can render, and that four Firebase API keys sit hardcoded across four separate projects in the production binary. Five further findings covered unrestricted device backup of browsing history and passwords, three undisclosed tracking SDKs, use of the browser's own privileged Topics API position for ad targeting, an undisclosed third-party VPN operator, and cryptocurrency wallet seed-phrase generation code sitting in the same process as the ByteDance-linked ad code.

Across 90 days and nine outbound messages, Opera's press and privacy inboxes returned automated acknowledgments throughout, and one human respondent, Michael Tegos, engaged twice with genuine technical content, on 15 September and again on 23 September 2026. Both replies disputed specific claims and neither answered any of the three yes-or-no questions the original disclosure asked, a pattern RFI-IRFOS's own Corporate Response Pattern Atlas documents as Pattern P-10, the Substituted Question: the underlying facts get engaged, and the specific question asked is not.

This report corrects one of RFI-IRFOS's own claims: the original disclosure named Kunlun Tech Co. Ltd and Qihoo 360 Security Technology Co. as Opera Software AS's PRC-incorporated majority shareholders since 2016. Opera's 23 September reply correctly points out that Qihoo 360, via its holding vehicle Qifei International, sold its entire 20.6% stake back to Opera in October 2022 and has not been a shareholder since. RFI-IRFOS independently verified this against Opera's own investor relations press release dated 17 October 2022 and accepts the correction. Kunlun Tech remains Opera's largest shareholder and is independently PRC-incorporated; the National Intelligence Law exposure this report describes rests on Kunlun Tech alone, not on two entities as originally stated.

All eight findings were re-scored under CVSS v4.0 for this closure report, not carried forward with the original hand-assigned labels. None reaches CRITICAL on a proper derivation. C1, the Pangle/ownership finding, has a CVSS v4.0 base of MEDIUM, 6.9, held at HIGH in this report under an explicit blast-radius escalation given Opera's very large global user base and the genuine, Kunlun-Tech-specific National Intelligence Law exposure that Opera's own EU/EEA geofencing claim does not resolve, a remotely configurable flag is not the same as a durable technical control, and this report does not have visibility into which one it actually is. C2 and C3 score MEDIUM, 6.9. H1 scores MEDIUM, 5.2. H2 scores MEDIUM, 6.9. H3, H4, and H5 are documented as structural and transparency findings, none was demonstrated as an independently exploitable attack path, and CVSS does not fit a disclosure-and-consent-architecture critique of this kind well.

Scope: Root-level static analysis of the production Opera Browser Android application (com.opera.browser, version 99.3.5094.89092), covering the AndroidManifest, resource strings, and decompiled dex, as pulled and reviewed on 25 June 2026. No dynamic instrumentation, live traffic capture, or interaction with Opera's backend infrastructure was performed. RFI-IRFOS was unable to pull a fresh production build for this closure report; Opera's own 23 September reply states several architectural changes (consent-enforcement mechanisms, EU/EEA geofencing, Google's MobileAdsInitProvider removal) that this report has not independently verified against a current binary, and that gap is stated here explicitly, it is not left implicit.

Disposition

Eight findings were disclosed on 25 June 2026: a ByteDance/Pangle ad SDK compiled into the browser inside a company with a PRC-domiciled major shareholder (C1), pre-consent ad-system initialization via ContentProvider auto-init (C2), four hardcoded Firebase API keys across four projects (C3), unrestricted device backup of browsing history and saved passwords (H1), three undisclosed third-party tracking SDKs (H2), a browser using its own privileged Topics API position for ad targeting (H3), an undisclosed third-party VPN operator behind the built-in free VPN (H4), and cryptocurrency wallet seed-phrase generation code co-located in the same process as the ByteDance-linked ad SDK (H5). Opera engaged twice with technical substance, on 15 September and 23 September 2026, disputing several points, and both times answered none of the three yes-or-no questions the original disclosure asked. Opera's second reply also corrected a factual error in RFI-IRFOS's own disclosure regarding a former shareholder, which this report accepts and corrects. This report closes and publishes the case on the terms stated from the first message: fixed 90-day coordinated disclosure, independent of engagement quality.

ID	Severity	Title
C1	HIGH	ByteDance/Pangle Ad SDK Compiled Into a Browser With PRC-Incorporated Ownership
C2	MEDIUM	Ad System ContentProvider Auto-Initialization, Consent Timing Unconfirmed
C3	MEDIUM	Four Hardcoded Firebase API Keys Across Four Projects
H1	MEDIUM	Unrestricted Device Backup of Browsing History and Saved Passwords
H2	MEDIUM	Three Undisclosed Third-Party Tracking SDKs in a Browser That Markets an Adblocker
H3	OBSERVATIONAL	ACCESS_ADSERVICES_TOPICS Held by the Same Browser That Blocks Third-Party Trackers
H4	OBSERVATIONAL	Free Built-In VPN Operated by an Undisclosed Third Party
H5	OBSERVATIONAL	Cryptocurrency Wallet Seed-Phrase Generation Co-Located With ByteDance-Linked Code

Subject & Operator Analysis

Opera Browser for Android is operated by Opera Norway AS, headquartered in Oslo, Norway, part of the Opera group of companies, publicly listed on NASDAQ as Opera Limited (OPRA). Opera is subject to Norwegian and EU/EEA law, with the Norwegian Datatilsynet as lead supervisory authority. Opera's shareholder base includes Kunlun Tech Co. Ltd, a PRC-incorporated entity and Opera's largest shareholder, among thousands of public shareholders following Opera's NASDAQ listing.

Opera maintains dedicated security and privacy contact channels (security@opera.com, privacy@opera.com), a Bugcrowd-hosted bug bounty program, and Michael Tegos, Product Marketing Manager for Privacy and Security, engaged directly and substantively twice across this case, the only human respondent RFI-IRFOS heard from in 90 days. Opera also identified a factual error in RFI-IRFOS's own original disclosure, and this report addresses it directly instead of leaving it standing.

Architecture & Data Flow

The Opera Browser Android production APK (version 99.3.5094.89092 at disclosure) compiles ByteDance's Pangle ad SDK as a first-class component, initializes its ad system and crash reporter via ContentProviders that the Android platform runs before any user-facing screen, ships four hardcoded Firebase credentials across four projects, allows unrestricted device backup of browsing data, and bundles three additional third-party tracking SDKs alongside a marketed adblocking feature. A built-in VPN and a cryptocurrency wallet are also present, operated and architected in ways this report documents as separate findings.

Findings

C1: ByteDance/Pangle Ad SDK Compiled Into a Browser With PRC-Incorporated Ownership

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. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because of the browser's very large global user base and the unresolved question of whether Opera's stated EU/EEA geofencing is a durable technical control or a remotely reversible flag.

The production APK compiles ByteDance's Pangle ad SDK as a first-class component (com.opera.android.ads.pangle.PangleAdsModuleImpl, com.bytedance.sdk.pangle, com.bytedance.sdk.openadsdk), with dedicated feed ad-unit formats and landing-page activities registered in the manifest. At the time of the original disclosure, Opera Software AS's shareholding included Kunlun Tech Co. Ltd and Qihoo 360 Security Technology Co., both PRC-incorporated. Correction made in this report: Qihoo 360's holding vehicle, Qifei International, sold its full 20.6% stake back to Opera in October 2022, independently verified against Opera's own investor relations release of that date, and is no longer a shareholder. Kunlun Tech remains Opera's largest shareholder and remains independently PRC-incorporated, so the National Intelligence Law Art. 7 exposure this finding describes now rests on that single relationship, not two. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because of the browser's very large global user base and the unresolved status of the EU/EEA restriction as a durable technical control versus a remotely reversible flag.

```
com.opera.android.ads.pangle.PangleAdsModuleImpl
com.bytedance.sdk.pangle (full SDK)
com.bytedance.sdk.openadsdk
bytedanceglobal_int

Manifest activities: TTCeilingLandingPageActivity, TTLandingPageActivity,
TTPlayableLandingPageActivity, TTVideoLandingPageLink2Activity
```

Opera's 23 September 2026 reply states the Pangle SDK is not available to EU/EEA users and that browsing data is not transferred to ByteDance. RFI-IRFOS's finding was never that Pangle is active for EU users today, it is that the compiled component and the ownership structure both exist in the shipped binary regardless of any remote feature flag governing runtime activation. A server-side geofence is not verifiable from outside the company and can change without a new release. Opera's reply does not state whether the EU/EEA restriction is enforced by a durable technical control (for example, a build-time exclusion) or a remotely configurable flag, and RFI-IRFOS asked this question directly on 15 September 2026. It remains unanswered.

Impact: If the EU/EEA restriction turns out to be a remotely reversible flag and not a build-time exclusion, EU user data could become reachable by Pangle without any new app release, at a time and to a degree RFI-IRFOS cannot detect from outside the company. Independent of geofencing, Kunlun Tech's PRC domicile and the corresponding National Intelligence Law obligations remain a standing governance fact about the company operating the browser.

Fix: State explicitly and demonstrably whether the EU/EEA Pangle restriction is enforced by a build-time technical control or a remote flag, and if the latter, move to a build-time control. No confirmation of either was ever received.

C2: Ad System ContentProvider Auto-Initialization, Consent Timing Unconfirmed

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.

com.opera.ads.internal.OperaAdsInitProvider is registered as a ContentProvider, which the Android platform initializes before Application.onCreate() and before any Activity, including any consent screen, by lifecycle design. com.opera.android.BreakpadInitProvider carries the maximum possible init order (0x7fffffff). Four BOOT_COMPLETED receivers additionally auto-start app components at device boot.

Opera's 23 September reply states that Google's MobileAdsInitProvider has been explicitly removed and that ad initialization occurs only after the relevant consent flow. RFI-IRFOS's finding never named MobileAdsInitProvider, it named OperaAdsInitProvider specifically. Confirming that a Google-provided class was removed does not confirm whether Opera's own OperaAdsInitProvider gates its ContentProvider onCreate() behind a consent check, the specific question RFI-IRFOS asked directly on 15 September 2026. It remains unanswered.

Impact: A ContentProvider's onCreate() runs before the user has seen any part of the application, including a consent screen. Whether the code inside OperaAdsInitProvider's onCreate() performs consent-gated initialization internally cannot be determined from the manifest entry alone, and Opera has not confirmed it either way.

Fix: Confirm, with the specific code path or config check, that OperaAdsInitProvider's ContentProvider onCreate() itself gates any advertising-related initialization behind a recorded consent state, not merely that ad delivery is gated at a later point.

C3: Four Hardcoded Firebase API Keys Across Four Projects

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

Four distinct Firebase API keys, corresponding to six Firebase app IDs across four separate projects, are extractable from the production binary with the 'strings' command. Opera's 23 September reply states that Firebase API keys are not authentication credentials and that access control is enforced through Firebase Security Rules, App Check, and server-side validation, in general terms, not per key.

That framing answers a confidentiality question, not a security one. RFI-IRFOS's 15 September reply asked Opera to confirm App Check is enforced on all four keys individually, not asserted as a general practice, since without it a backend cannot distinguish the genuine app from a replayed key. That confirmation, per key, was never given. With four keys across four projects, the residual risk compounds across a correspondingly larger surface: quota or billing exhaustion, unrestricted-key replay against other Google APIs, and project/sender-ID enumeration are each possible against any one of the four independently.

Impact: Four separate Firebase projects each carry independent quota-exhaustion and key-replay risk, without per-key confirmation that App Check or equivalent controls are actually enforced on each.

Fix: Confirm App Check enforcement individually for all four keys, or rotate and restrict each by package name and signing certificate at minimum.

H1: Unrestricted Device Backup of Browsing History and Saved Passwords

MEDIUM, CVSS v4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 5.2.

AndroidManifest.xml declares android:allowBackup="true" with no backup-rules file excluding any data category. For a browser, this means the full browsing history, saved passwords, cookies, bookmarks, and cached credentials are eligible for Android's automatic backup service, which for most users means Google's cloud infrastructure, a US company subject to the US CLOUD Act.

Impact: Anyone with access to a user's Google account or a backup-capable ADB connection to the device can retrieve the full backed-up dataset, including saved passwords, without needing to compromise the browser itself.

Fix: Declare a backup-rules file excluding browsing history, saved credentials, and cookies from the automatic backup set, or disable allowBackup entirely for a privacy-focused browser. No confirmation that this has occurred was ever received.

H2: Three Undisclosed Third-Party Tracking SDKs in a Browser That Markets an Adblocker

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.

AppsFlyer (attribution and behavioral tracking), Leanplum/CleverTap (push and behavioral analytics, including a location-accuracy enum), and the Facebook SDK are all compiled into a browser that separately ships and markets Adblock Plus as a user-facing privacy feature. Each is a distinct data processor under GDPR Art. 28.

Impact: A browser blocking third-party trackers on behalf of the user while running three of its own undisclosed third-party trackers is a direct contradiction between the marketed feature and the actual data flows, independent of any single technical severity rating.

Fix: Name all three processors explicitly in the privacy policy with their specific purposes, and confirm signed Art. 28 DPAs are in place for each. No confirmation that this has occurred was ever received.

H3: ACCESS_ADSERVICES_TOPICS Held by the Same Browser That Blocks Third-Party Trackers

OBSERVATIONAL, not independently CVSS-scored, this is a disclosure and design-conflict finding, not a demonstrated technical attack path.

The Google Topics API (android.permission.ACCESS_ADSERVICES_TOPICS) is designed to replace third-party cookies with privacy-preserving interest signals, controlled by the browser itself. Opera holds this permission while simultaneously shipping Adblock Plus and the Pangle ad network. Using a privileged, browser-level API position to generate ad-targeting signals for the browser's own ad network, on the same interest profile the API exists to protect, is a design conflict worth naming on its own, separate from whether it is CVSS-scoreable.

Impact: Not independently assessed; this finding describes a policy and product-design tension, not a confirmed exploit path.

Fix: Disclose explicitly how Topics API data is used relative to the browser's own ad network, if at all.

H4: Free Built-In VPN Operated by an Undisclosed Third Party

OBSERVATIONAL, not independently CVSS-scored, this is a transparency finding, not a demonstrated technical attack path.

Opera's built-in free VPN routes through KAPE Technologies infrastructure (com.kape.vpnservicemanager, formerly Crossrider, now the owner of Private Internet Access), not Opera's own infrastructure, and this is not disclosed in the browser's user interface at the point a user enables the feature.

Impact: Users who enable the VPN believing their traffic stays within Opera's own control are, in practice, trusting a separate, US-linked VPN operator without being told.

Fix: Disclose the actual operator of the VPN service at the point of activation, not only in a privacy policy few users read.

H5: Cryptocurrency Wallet Seed-Phrase Generation Co-Located With ByteDance-Linked Code

OBSERVATIONAL, not independently CVSS-scored, this is a static code-colocation observation, not a confirmed exfiltration finding.

Opera ships a full Celo blockchain wallet (celopay), including seed-phrase generation, within the same application process that executes the ByteDance/Pangle ad code described in C1. RFI-IRFOS's original disclosure stated explicitly that this is not an allegation of active exfiltration, it is a documented code co-location that a security architecture built with this risk in mind would not permit.

Impact: Not independently assessed as an active exploit; the architectural observation stands regardless of whether any cross-component data access has occurred.

Fix: Isolate cryptographic key-material generation into a separate, sandboxed process from any third-party ad SDK, independent of whether current behavior is provably safe.

Withdrawn and Corrected Claims

RFI-IRFOS's original disclosure and every follow-up through 15 September 2026 named Kunlun Tech Co. Ltd and Qihoo 360 Security Technology Co. together as Opera Software AS's PRC-incorporated majority shareholders since 2016. This was accurate at the time of the 2016 acquisition and is no longer accurate. Opera's 23 September 2026 reply states that Qihoo 360's holding vehicle sold its entire stake back to Opera and has not been a shareholder since 2022. RFI-IRFOS independently verified this against Opera's own investor relations press release, dated 17 October 2026 (Oslo), confirming the repurchase of 360's full 46.75 million shares, a 20.6% stake, with 360 stated as no longer a shareholder. This correction is made here directly, it is not left standing on the public record. It narrows, and does not eliminate, finding C1: Kunlun Tech remains Opera's largest shareholder and remains independently PRC-incorporated.

Impact Analysis

The findings in this report sort into two groups with different practical weight. C1 through C3 describe a compiled, third-party-obligated ad SDK initializing early in the application lifecycle inside a company with a standing PRC ownership relationship, alongside hardcoded credentials, all independently verifiable from the shipped binary. H1, H2, H3, and H4 describe a consistent pattern across the same product: a browser that markets privacy features (an ad-blocker, a free VPN) while running undisclosed tracking, unrestricted backup, and privileged-API ad targeting underneath those same marketed features. H5 sits alongside C1 as an architectural observation about where sensitive code lives relative to the ByteDance-linked component, not a separate technical claim.

Pattern P-10, The Substituted Question

Both of Opera's substantive replies, 15 September and 23 September 2026, engaged real technical and factual content and answered none of the three yes-or-no questions the original disclosure asked. This is documented in the RFI-IRFOS Corporate Response Pattern Atlas v0.1 as Pattern P-10, the Substituted Question: the underlying facts are conceded or disputed in detail, while the specific legal question built on top of them, DPO awareness, an Art. 44 transfer mechanism, or a removal date, goes unanswered both times. Opera is the clearest repeat instance of this pattern RFI-IRFOS has recorded in this campaign, the same structure appearing twice, four months apart, across two different named respondents at the same company.

Article	Finding	Basis

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. 44-49	C1	International transfer mechanism for any EU browsing data reachable by a PRC-domiciled ad network, contingent on whether the EU/EEA restriction is a durable technical control.
Art. 7, Art. 25	C2	Consent must precede processing, and privacy-by-design requires that a ContentProvider auto-initializing before any consent screen not perform consent-relevant initialization internally.
Art. 5(1)(f), Art. 32	C3	Security of processing for four hardcoded, unrotated project credentials.
Art. 5(1)(f), Art. 32	H1	Unrestricted backup of browsing history and credentials to third-party cloud infrastructure.
Art. 13(1)(e), Art. 28	H2	Three undisclosed data processors requiring named disclosure and signed processing agreements.

Regulatory & Legal Landscape

Opera Software AS is incorporated in Norway, an EEA member state applying GDPR in full, with the Norwegian Datatilsynet as lead supervisory authority. Opera Limited's NASDAQ listing (OPRA) and its large, PRC-incorporated shareholder subject the parent group to disclosure obligations and investor scrutiny independent of, and in addition to, its GDPR exposure. The Austrian DSB and CERT.at were held in BCC across this case's correspondence from the first message.

IOC / Reproducible Evidence

```
Package: com.opera.browser
Version at disclosure: 99.3.5094.89092

C1: com.opera.android.ads.pangle.PangleAdsModuleImpl, com.bytedance.sdk.pangle,
    com.bytedance.sdk.openadsdk
C2: com.opera.ads.internal.OperaAdsInitProvider, com.opera.android.
    BreakpadInitProvider
    (initOrder=0x7fffffff)
C3: four Firebase API keys, six app IDs, four projects (extractable via `strings`)
H1: android:allowBackup="true", no backup-rules exclusions
H2: com.appsflyer.*, com.leanplum.*, com.facebook.*
H3: android.permission.ACCESS_ADSERVICES_TOPICS
H4: com.kape.vpnservicemanager.*
H5: assets/composeResources/com.opera.celopay.model.crypto.generated.resources/
    files/mnemonic_vocabulary.txt
```

No fresh production build was pulled for this closure report. RFI-IRFOS does not independently know whether the architectural changes described in Opera's 23 September reply, consent-enforcement mechanisms, EU/EEA geofencing, or MobileAdsInitProvider removal, are present in the current Google Play build, and states that gap explicitly instead of assuming continuity in either direction.

Disclosure Timeline & Outcome

Date	Event
2026-06-25	R1 sent to Opera's DPO channel and press team, eight findings, three yes/no questions, 90-day embargo set for 2026-09-23.
2026-06-27 through 2026-08-09	Four further follow-ups, each answered only by automated press or privacy acknowledgments.
2026-08-11	First human reply, Michael Tegos, procedural only: confirms correct channels, commits to follow up.
2026-09-06	Follow-up restating the three questions, deadline 13 September 2026.
2026-09-15	First substantive technical reply from Opera, disputing several points, answering none of the three questions.
2026-09-15	RFI-IRFOS response crediting the engagement, rebutting each disputed point with specific evidence, restating the three questions, deadline 19 September 2026.
2026-09-23	Second substantive reply, corrects RFI-IRFOS's Qihoo 360 shareholder claim, disputes further points, again answers none of the three questions.
2026-09-23	Case closed and published, on the original embargo date.

Nine outbound messages, two genuine technical replies from one named respondent, zero yes-or-no answers to the three original questions across either reply, and one real, credited correction to RFI-IRFOS's own claim. That is the full record this case closes on.

Residual Risk & Recommendations

The three original questions remain open at publication: whether Opera's DPO is aware of Pangle's pre-consent initialization pathway, whether a valid Art. 44 transfer mechanism covers any EU data reachable by ByteDance, and whether Pangle will be removed or consent-gated at the binary level and by which date. RFI-IRFOS recommends, in order: confirm whether the EU/EEA Pangle restriction is a build-time control or a remote flag, and make it the former (C1); confirm whether OperaAdsInitProvider's own ContentProvider onCreate() gates advertising-relevant initialization behind consent (C2); confirm App Check enforcement individually on all four Firebase keys (C3); exclude browsing history and credentials from automatic device backup (H1); and name AppsFlyer, Leanplum, and Facebook explicitly as processors with signed DPAs (H2). Weekly monitoring of the public build continues after this publication; any change to any finding, including confirmation of the architectural claims in Opera's own replies, will be documented and added to the public record.

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, exactly as C1 is escalated in this report. Three findings (H3, H4, H5) are documented as structural or transparency observations, for the same reason, CVSS does not fit every real finding, and forcing a score onto one it does not describe well is its own kind of inaccuracy. Disclosure conducted under ISO/IEC 29147 and the Austrian Forschungsfreiheitsgesetz, Art. 17 StGG. REF OPERA-2026-R1.