Coordinated Security & Privacy Disclosure, Final Report

Nintendo Switch Online (com.nintendo.znca) + Nintendo Store (com.nintendo.znej)

Family-console companion apps, a bug-bounty redirect, a decline letter naming zero findings, three standing questions on children's voice and location data never answered

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – NINETY DAYS, A DECLINE LETTER, ZERO FINDINGS NAMED

Target	Nintendo of Europe SE, Frankfurt am Main, Germany
Products audited	Nintendo Switch Online (com.nintendo.znca v3.4.0), Nintendo Store (com.nintendo.znej v3.2.0)
Disclosure reference	REF NINTENDO-2026-R1, Incident 260621-002328
R1 sent	2026-06-21
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (NSO C1 / Store C1, hardcoded Firebase keys, CVSS v4.0 9.3)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 21 June 2026, RFI-IRFOS performed static analysis of Nintendo Switch Online and Nintendo Store, two companion apps to a family gaming console, and identified eight findings, three CRITICAL, three HIGH, two further, across the two applications. The most significant, in RFI-IRFOS's assessment: VoiceChatService, backed by RECORD_AUDIO and FOREGROUND_SERVICE_MICROPHONE, is active on Nintendo Switch Online family accounts used by minors, and 1,029 Salesforce Marketing Cloud smali files in Nintendo Store include a LocationReceiver processing GPS check-in data tied to child family-group accounts.

Two hardcoded Firebase API keys were extracted verbatim from the two apps' production binaries, along with a hardcoded, unrestricted Google Maps API key in Nintendo Store, the only app in RFI-IRFOS's 2026 audit series found carrying two publicly extractable API keys.

Nintendo's Contact Center Europe redirected the disclosure to its HackerOne bug bounty program on 24 June, addressing no specific finding. On 24 August, Nintendo's Privacy Team sent a letter declining what it characterized as an unsolicited EUR 100,000 advisory-services offer, stating an internal technical and privacy review found the claims 'largely inaccurate' without identifying which finding it disputed or why, and declaring the matter closed while urging RFI-IRFOS to refrain from further contact. RFI-IRFOS's point-by-point response of the same day restated all eight findings by name and three specific standing questions on children's data; none has been answered.

Scope: Static analysis of two publicly downloaded production Nintendo Android APKs, on an authorized test device, only. No Nintendo account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 21 June 2026 to dataprotectionofficer@nintendo.de, cc privacyinquiry.noe@nintendo.de, eight findings across two applications. Nintendo of Europe's Contact Center redirected to its HackerOne bug bounty program on 24 June, addressing no specific finding. On 24 August, Nintendo's Privacy Team sent a letter declining what it characterized as 'an offer for advisory services in connection with payment of EUR 100,000,' asserting an internal review found the claims 'largely inaccurate' without naming a single one of the eight findings, and stating the matter closed. Three standing questions on the legal basis for RECORD_AUDIO and location processing on minors' accounts, DPO awareness, and DPIA existence remain unanswered.

ID	Severity	Title
NSO-C1	CRITICAL	Hardcoded Firebase API key, Nintendo Switch Online, project nsd-coral-prod
NSO-H1	HIGH	No network security configuration: Nintendo Account authentication and voice-chat signaling unpinned
NSO-H2	HIGH	VoiceChatService with RECORD_AUDIO and FOREGROUND_SERVICE_MICROPHONE active on family accounts used by minors

ID	Severity	Title
Store-C1	CRITICAL	Hardcoded Firebase API key, Nintendo Store, project nsd-entry-lp1
Store-C2	CRITICAL	Hardcoded, unrestricted Google Maps API key
Store-H1	HIGH	Salesforce Marketing Cloud LocationReceiver: GPS check-in data tied to child family-group accounts, processor undisclosed

Subject & Operator Analysis

Nintendo of Europe SE (Frankfurt am Main, Germany) operates the two companion applications audited here for the Nintendo Switch, a console whose install base and marketing are substantially oriented toward families and children.

Positive Observations

- android:allowBackup=”false” is set in both applications.
- PairIP anti-tamper protection is present in Nintendo Switch Online.
- Minimal third-party advertising footprint: no Facebook SDK, no Adjust, no ad networks identified in either app.
- ZXing (Apache 2.0) is used cleanly with no modification concerns.
- Both Firebase projects are clearly named and internally organized, suggesting deliberate infrastructure practice even where credential hygiene fell short.

Findings

NSO-C1: Hardcoded Firebase API key, Nintendo Switch Online, project nsd-coral-prod

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

API key AIzaSyBZ22TShtFzEiWFH_ZxVQy-asoSjAeRfzw, project nsd-coral-prod, extracted from the public Play Store binary of an app with a reported 40M+ subscriber base.

```
Project:  nsd-coral-prod
API Key:  AIzaSyBZ22TShtFzEiWFH_ZxVQy-asoSjAeRfzw
DB URL:   https://nsd-coral-prod.firebaseio.com
```

Nintendo's 24 August letter states an internal review found RFI-IRFOS's claims 'largely inaccurate' without naming this or any other finding individually. This key, its presence in the public binary, and its project identifier are independently reproducible by any party downloading the same public APK; RFI-IRFOS's point-by-point response of 24 August requested Nintendo identify specifically which finding it disputes. No reply has done so.

Impact: A publicly extractable key in an app with a large subscriber base enables forged push notifications, Firebase database and storage probing, and remote-config manipulation, subject to whatever backend security rules Nintendo has not disclosed.

Fix: Rotate the credential, publish the project's security-rules configuration, and restrict the key to the production certificate fingerprint.

NSO-H1: No network security configuration: Nintendo Account authentication and voice-chat signaling unpinned

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

No android:networkSecurityConfig is declared in either app. Nintendo Account authentication and VoiceChatService signaling rely on Android platform TLS defaults only, with no certificate pinning.

Not individually addressed in any Nintendo reply.

Impact: An actor with a system-trusted CA certificate on the device can intercept authentication tokens and voice-chat signaling metadata.

Fix: Implement a network security configuration with certificate pinning for Nintendo Account authentication and voice-chat signaling endpoints.

NSO-H2: VoiceChatService with RECORD_AUDIO and FOREGROUND_SERVICE_MICROPHONE active on family accounts used by minors

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

com.nintendo.znca.core.services.voip.VoiceChatService, declared with RECORD_AUDIO, FOREGROUND_SERVICE_MICROPHONE, and MODIFY_AUDIO_SETTINGS, is a legitimate feature for titles including Splatoon 3 and Animal Crossing. The Nintendo Switch is a family console, and many NSO subscribers are minors using family accounts.

RFI-IRFOS's finding, as originally stated, is not that voice chat should not exist, but that voice data from children under 13 is COPPA-covered content (16 CFR 312) and that EU child accounts engage GDPR Art. 8, and that no age-appropriate consent flow specific to this service was identified. Nintendo's 24 August letter does not name this finding. RFI-IRFOS's standing question, restated in every follow-up through 3 September and unanswered: what is the legal basis, under Art. 6/7 and Art. 8 given minors' accounts, for RECORD_AUDIO access, and what age-appropriate consent flow governs it?

Impact: Voice data from children using family accounts may be processed without a confirmed, age-appropriate consent mechanism, engaging COPPA and GDPR Art. 8 directly.

Fix: Publish the specific consent flow governing VoiceChatService activation for accounts flagged as belonging to a minor, and confirm whether a DPIA under Art. 35 covers this feature.

Store-C1: Hardcoded Firebase API key, Nintendo Store, project nsd-entry-lp1

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

API key AIzaSyBEuaqhVwPZGUbz-TOQybQuGweCgMFyEvo, project nsd-entry-lp1, extracted from the public Play Store binary of Nintendo's loyalty and event check-in platform.

Not individually named in Nintendo's 24 August letter.

Impact: A publicly extractable loyalty-platform credential enables probing of check-in databases, forged push notifications, and manipulation of event configs and point balances.

Fix: Rotate the credential and restrict it to the production certificate fingerprint.

Store-C2: Hardcoded, unrestricted Google Maps API key

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N, 8.7

API key AIzaSyA7PL3laHgvp5U8wlGUINH5sgW46CH8r6c, sourced from res/values/strings.xml, billing against Nintendo's own Google Cloud account, with no confirmed restriction to package name and SHA-256 signing fingerprint.

Across 14 apps audited in this bundle of the research series, Nintendo Store is the only application found carrying two independently, publicly extractable API keys. Not individually named in Nintendo's 24 August letter.

Impact: An unrestricted, publicly extractable Maps key enables quota-exhaustion billing abuse against Nintendo's own cloud account.

Fix: Restrict the key to the package name plus SHA-256 signing fingerprint, and scope it to the Maps SDK only.

Store-H1: Salesforce Marketing Cloud LocationReceiver: GPS check-in data tied to child family-group accounts, processor undisclosed

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

1,029 Salesforce Marketing Cloud smali classes, including com.salesforce.marketingcloud.location.LocationReceiver, process GPS coordinates and timestamps from Nintendo event check-ins. res/values/strings.xml includes the string "mypage_checkin_child_description": "child accounts that are part of your family group", confirming the check-in flow covers child accounts specifically, including check-ins performed by a parent scanning a QR code on a child's behalf.

RFI-IRFOS's finding: Salesforce Inc. (San Francisco, California) is not named as a processor for this data in Nintendo's EU privacy notice, to RFI-IRFOS's knowledge. Nintendo's 24 August letter does not name this finding. RFI-IRFOS's point-by-point response of 24 August states, verbatim: '1,029 Salesforce Marketing Cloud smali files including an active LocationReceiver processing GPS check-in data tied to child family accounts are not marketing content. They are precisely what dataprotectionofficer@nintendo.de exists to receive.'

Impact: GPS location data tied to child family-group accounts is processed by an undisclosed US third-party processor with no confirmed Art. 46 transfer safeguard.

Fix: Name Salesforce Inc. as a processor for this data flow in the applicable EU privacy notice, publish the Art. 46 transfer mechanism, and confirm whether an Art. 35 DPIA covers child-account location processing specifically.

Nintendo’s Response, Recorded in Full

On 24 June 2026, Nintendo’s Contact Center Europe (support@nintendo.eu) replied to the original disclosure, in full: ”vielen Dank, dass Sie uns diesen Sicherheitslückenberich t zugesendet haben. Wir verfügen über ein offizielles Bug-Bounty-Programm in HackerOne, speziell zum Melden von Nintendo-Sicherheitsverwundbarkeiten und würden uns freuen, entsprechende Berichte dazu, über folgenden Link zu erhalten https://hackerone.com/ninte ndo.” No specific finding was referenced.

On 24 August 2026, Nintendo’s Privacy Team (privacyinquiry.noe@nintendo.de) sent the following, quoted in full and unedited: ”We respectfully decline your offer for advisory services in connection with payment of EUR 100,000. We urge you to refrain from (i) sending us any further unsolicited commercial communications, and (ii) disseminating false or misleading information regarding Nintendo’s products or services… your organisation chose to send unsolicited commercial communications to Nintendo’s Privacy team and Data Protection Officer, neither of which is an appropriate contact point for marketing correspondence or B2B solicitations… we conducted a thorough internal review of the smart device applications referenced, involving both our technical experts and privacy department. That review established that the claims in your email are largely inaccurate and do not result in the privacy-related consequences suggested by your email… We consider this matter closed.” Signed ”Nintendo Privacy Team,” no individual name given.

RFI-IRFOS’s characterization of its own 21 June message, restated in its 24 August point-by-point response: the EUR 100,000 figure was a deliverables-based technical remediation and advisory package, offered once at the end of the message, after all eight findings had already been disclosed in full technical detail, unconditionally, at no cost. It was not a marketing solicitation and was not conditioned on the findings’ delivery. RFI-IRFOS’s response also notes that it had already written, on 24 July, exactly one month before the decline letter, stating plainly it does not use HackerOne or bug bounty submission channels.

Nintendo’s letter does not identify which of the eight findings it considers inaccurate, or why. Every fact in the original disclosure, a Firebase key’s presence, the absence of a network security configuration file, and the presence of the named Salesforce smali classes, is independently verifiable from the same public binary by any third party. RFI-IRFOS’s three standing questions, restated in every follow-up through 3 September, remain unanswered: the legal basis under Art. 6/7 and Art. 8 for RECORD_AUDIO and the Salesforce Location-Receiver on minors’ accounts, whether Nintendo’s DPO was independently aware of these specific findings, and whether a documented Art. 35 DPIA covers processing on minors’ accounts.

Data Protection, Article by Article

Finding	Provision	Concern
NSO-C1	GDPR Art. 32(1); NIS2	Hardcoded, publicly extractable credential
NSO-H1	GDPR Art. 25, Art. 32(1)(a)	No certificate pinning, authentication and voice signaling unpinned
NSO-H2	GDPR Art. 6(1), Art. 8(1); COPPA 16 CFR 312	Background microphone service on minors' family accounts
Store-C1	GDPR Art. 32(1)	Hardcoded, publicly extractable credential
Store-C2	GDPR Art. 32(1)	Unrestricted, publicly extractable billing-linked key
Store-H1	GDPR Art. 13(1)(e), Art. 46, Art. 5(1)(c), Art. 8	Undisclosed US processor for child-account GPS data

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-21	R1 sent to dataprotectionofficer@nintendo.de, cc privacyinquiry.noe@nintendo.de, bcc DSB/CERT.at, 8 findings across 2 apps
2026-06-21	Automated auto-reply confirms receipt, incident 260621-002328
2026-06-24	Nintendo Contact Center Europe (support@nintendo.eu): templated HackerOne bug-bounty redirect, no finding referenced
2026-07-23 / 08-24	Follow-ups: '30 days, three automated replies, zero humans' and '64 days, two automated'
2026-08-24 10:15	Nintendo Privacy Team: decline letter, EUR 100,000 mischaracterized as an unsolicited commercial offer, internal review finds claims 'largely inaccurate' without naming a finding, matter declared closed
2026-08-24 10:50	RFI-IRFOS point-by-point response: all eight findings restated by name, three standing questions on children's voice and location data restated
2026-08-31 / 09-03	Further follow-ups; no further human reply received beyond automated ticket acknowledgments
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Across three months, Nintendo's only two non-automated replies were a templated bug-bounty redirect and a letter declining an offer it characterized as unsolicited commercial advisory services, asserting without specifics that an internal review found the claims largely inaccurate. No message from Nintendo, at any point, named, disputed with technical detail, or engaged individually with any of the eight findings, including the two involving children's voice and location data.

Residual Risk & Recommendations

- Answer, by name, which of the eight findings Nintendo’s internal review disputes and on what technical basis.
- Publish the consent flow and legal basis governing VoiceChatService for minors’ family accounts, and confirm Art. 35 DPIA coverage.
- Name Salesforce Inc. as a data processor for child-account GPS check-in data and publish its Art. 46 transfer mechanism.
- Rotate both Firebase credentials and the unrestricted Google Maps key across both applications.
- Implement certificate pinning for Nintendo Account authentication and voice-chat signaling.

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, 6, 8, 13, 25, 32, 35, 46; COPPA 16 CFR 312. REF NINTENDO-2026-R1.