Security & Privacy Disclosure, Final Report

connectgo.pro by ottobock. for Android (com.ottobock.pro.connectgo)

The clinician app that writes settings to a patient's prosthetic leg: a sign-in redirect to harden, staging traces in production and a Data Safety card that leaves out the patient.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED 20 NOVEMBER 2026. NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026.

Target	Ottobock SE & Co. KGaA, with Otto Bock Healthcare Products GmbH, Vienna as manufacturer and support entity
Versions Audited	2.1.0 / 95209 (analysis 2026-08-22)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days, unchanged)
Findings	4: 1 Medium, 3 Low (M1, M2 and M3 reassessed from Medium)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`c67c3f3379f4faf777311f33cdab4522d919bb651dfd83837ecf96deecc9fc8f`

security@rfi-irfos.com • rfi-irfos.com

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

Contents

1 Executive Summary 3

2 Finding Status at a Glance 4

3 Subject & Operator Analysis 4

4 Architecture & Data Flow 5

5 Findings 6
- 5.1 M1: OAuth redirect activity ships both a staging and a production URI scheme, exported, without host restriction 6
- 5.2 M2: Internal backend codename and a partial staging hostname inside the shipped binary 7
- 5.3 M3: No app-specific privacy policy link found through the Play listing 7
- 5.4 M4: Patient configuration data is not represented in the Data Safety declaration 8

6 Impact Analysis 8

7 The Complete Chain 9

8 Version Blocklist as Remote-Configuration Capability 9

9 Medical Device Context 10

10 Data Protection: Article by Article 10

11 Regulatory & Legal Landscape 10

12 Indicators of Compromise & Reproducible Evidence 11

13 Disclosure Timeline & Outcome 11

14 What Ottobock Got Right 12

15 Residual Risk & Recommendations 12

Executive Summary

connectgo.pro by ottobock. is the app that orthotics and prosthetics professionals use to install, calibrate and reconfigure microprocessor-controlled Ottobock prostheses and orthoses over Bluetooth. It has 5,000 plus installations on Google Play. On 22 August 2026 RFI-IRFOS sent four findings from a root level code analysis of version 2.1.0 under REF CONNECTGOPROBYOTTOBOCK-2026-R1.

The app is cleaner than most apps in this programme. The binary contains no hardcoded keys, no advertising or session-replay SDKs and a minimal set of permissions. The findings are bounded. The exported OAuth redirect activity ships a production and a staging URI scheme, a configuration fragment names an internal backend codename and a partial staging host, no app-specific privacy policy could be reached through the store listing, and the Data Safety card describes the clinician only, although the app's purpose is to write settings to the device of a patient who never sees it.

The central question is not a numbered finding. It is whether the app's authorisation is checked on the server for every configuration write or only once at sign-in. The binary shows real identity federation and a single-use qualification certificate, which argues against a purely client-side boundary, and it does not show that each write is re-checked. That question needs the manufacturer's answer.

Three of the four severities sent in the first notice are lowered in this report. Ottobock sent no substantive reply to the first notice or to the two follow-ups of 12 September and 17 October 2026 or to the final notice of 15 November 2026.

Scope: Root level code analysis of the Google Play release 2.1.0 (versionCode 95209) as an XAPK obtained through a mirror and cross-checked against the live listing: manifest, resources, two dex shim files and string-level extraction from the assembly store. No IL decompilation was done. No Ottobock server or account was contacted, no device was paired and no command was sent. Dynamic analysis is not part of this report.

ID	Severity	Title
M1	LOW	OAuth redirect activity ships both a staging and a production URI scheme, exported, without host restriction
M2	LOW	Internal backend codename and a partial staging hostname inside the shipped binary
M3	LOW	No app-specific privacy policy link found through the Play listing
M4	MEDIUM	Patient configuration data is not represented in the Data Safety declaration

Finding Status at a Glance

The table shows the severity sent in the first notice of 22 August 2026 next to the severity in this report. The notice asserted no Critical or High finding, and none is asserted here. Three of the four findings are rated lower here, because the evidence supports a lower band than the notice stated.

ID	Sent 22 Aug 2026	This report	Basis
M1	MEDIUM	LOW	Likely PKCE mitigation, CVSS 1.8.
M2	MEDIUM	LOW	Name disclosure, full hostname not available, CVSS 0.0.
M3	MEDIUM	LOW	Policy may exist at an unguessed address, CVSS 0.0.
M4	MEDIUM	MEDIUM	Editorial rating with reason stated in the finding, CVSS 0.0.

Subject & Operator Analysis

connectgo.pro by ottobock. is the app for orthotics and prosthetics professionals. They use it to install, calibrate and reconfigure microprocessor-controlled lower-limb prostheses and orthoses over Bluetooth: standard behaviour settings, MyModes movement-pattern profiles, static calibration and optimisation, and status readout. The developer of record on Google Play is Ottobock SE & Co. KGaA. The manufacturer and support entity named on the listing is Otto Bock Healthcare Products GmbH, Brehmstraße 16, 1110 Wien, Austria, telephone +43 1 523 37 86, fax +43 1 523 22 64. Both are EU or EEA entities, so no Article 27 representative gap applies. The store shows 5,000 plus installations and a PEGI 3 rating, and the listing carries the note ”For qualified personnel”.

Item	Value
Package	com.ottobock.pro.connectgo
Version	2.1.0 (versionCode 95209)
Base APK SHA-256	c67c3f3379f4faf777311f33cdab4522d919bb651dfd83837ecf96deecc9fc8f (72,554,501 bytes)
XAPK SHA-256	a00104ab0e17b23e153228698762f45ed284bcb5f82b8d703408080af0d17a67 (169,967,653 bytes, base, arm64-v8a, en, fr and hdpi splits)
minSdk / targetSdk	31 (Android 12) / 35 (Android 15)
Code base	.NET MAUI on Mono. classes.dex and classes2.dex hold 12,516 shim classes and no business logic. The application is in lib/arm64-v8a/libassemblies.arm64-v8a.blob.so, 80.3 MB, XABA v2 store with 250 local and 500 global entries

Item	Value
Source of the package	APKPure mirror. Package, version and developer were cross-checked against the live Google Play listing, and the XAPK hash matches the hash published by the mirror
Contacts	connectgo.pro@ottobock.com (found in the app's own localised consent strings), apps@ottobock.com (Play developer contact), myottobock@ottobock.com (Play listing contact)
App-specific privacy policy	not found through the Play listing (UNVERIFIED, see M3)
Data protection officer	not found through the channels checked (UNVERIFIED)

Supervisory competence: the manufacturer and support entity named on the listing is Austrian, which makes the Datenschutzbehörde the working candidate. Ottobock SE & Co. KGaA has its headquarters in Duderstadt, Lower Saxony, so the Landesbeauftragte für den Datenschutz Niedersachsen could be the lead authority under Article 56. That determination depends on the internal controller structure and is UNVERIFIED.

Architecture & Data Flow

The application logic is compiled .NET in a single assembly store inside an ELF container. No assemblies.manifest ships in this release build, so assembly names could not be resolved from a manifest. Findings that rest on the store are string-level evidence. No .NET decompiler was available, and claims that would need IL reading are marked UNVERIFIED.

Layer	Observed	Source
Sign-in	Microsoft identity platform (MSAL) with a redirect through BrowserTabActivity. Localised strings describe a single-use qualification certificate	AndroidManifest.xml, assembly store strings
Device commands	Capability interface UopDevice ISliderRead and the assembly name Ottobock.Caa.ViennaRemoting.UNE.dll, the same Ottobock.Caa device framework as the sibling apps	assembly store strings
Backend	Codename GlamApi with a partial staging host value	assembly store strings
Version gate	Bundled blocklist for app and OS versions	assets/VersionCheck/version_blacklist.json
Telemetry	New Relic Mobile inside Ottobock.Caa.Analytics.Maui assemblies, the only third-party SDK	assembly store strings

The sibling notice for connectgo (REF OTTOBOCKCONNECTGO-2026-R1, sent on the same day) reported that this app's native library set contains libe_sqlite3.so and no SQLCipher

provider. That observation reached Ottobock in writing on 22 August 2026. It is not repeated here as a numbered finding, because the material in this report folder does not hold its evidence.

Findings

M1: OAuth redirect activity ships both a staging and a production URI scheme, exported, without host restriction

LOW, CVSS v4.0 AV:L/AC:H/AT:P/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 1.8 (CVSS-B), disclosed as MEDIUM on 22 August 2026, reassessed in this report

The exported BrowserTabActivity registers the custom schemes connectgopro-staging and connectgopro. This is the standard redirect catcher for an MSAL sign-in. A custom URI scheme cannot be claimed exclusively, so another app on the same device can register the same scheme and receive the redirect intent. RFC 8252 names PKCE as the mitigation and current MSAL SDKs enable it by default. Whether PKCE is enforced end to end here was not verified, and the score assumes that it is. A second observation is that the staging scheme ships in the public production build.

```
<activity android:configChanges="orientation|screenSize" android:exported="true"
    android:name="crc648316b0a9aa8cfd61.BrowserTabActivity">
    <intent-filter>
        <action android:name="android.intent.action.VIEW"/>
        <category android:name="android.intent.category.BROWSABLE"/>
        <category android:name="android.intent.category.DEFAULT"/>
        <data android:scheme="connectgopro-staging"/>
        <data android:scheme="connectgopro"/>
    </intent-filter>
</activity>
```

microsoft.identity.client.AuthenticationActivity is also declared as exported elsewhere in the manifest. That is expected MSAL behaviour and not part of this finding.

The staging scheme doubles the registered intent-filter surface for no production benefit and shows that a staging environment exists. For anyone who probes the Entra ID app registrations that is reconnaissance value.

Impact: Clinicians who sign in with their Ottobock ID are the users affected, and through them the patients whose devices the clinician configures. If PKCE were not enforced, a malicious app on a clinician’s phone could take over the sign-in. The question to the manufacturer asks whether it is enforced.

Fix: Confirm PKCE enforcement for the redirect flow, remove the staging scheme from production builds, and consider claimed HTTPS redirects where the identity platform supports them.

M2: Internal backend codename and a partial staging hostname inside the shipped binary

LOW, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as MEDIUM on 22 August 2026, reassessed in this report

The compressed .NET assembly store holds a configuration-shaped JSON fragment with the codename GlamApi and a host value that starts with https://glam-api-sta and is cut at a compression block boundary. The full hostname is not available from the evidence. Whether the endpoint exists, is reachable or is called by the shipped build is UNVERIFIED. CVSS scores the disclosure of a name at 0.0.

```
"GlamApi
"Host": "https://glam-api-sta
```

The extracted value is truncated in the evidence. The complete value is not available in the evidence and is not reconstructed here. The pattern suggests a staging host, but that is an inference. Neither the codename nor a matching hostname appears in the store listing or in public product documentation.

Impact: The finding carries no direct consequence for clinicians or patients. It shows what a production build contains that a production build does not need.

Fix: Remove staging configuration from production builds and keep staging hostnames out of release artefacts.

M3: No app-specific privacy policy link found through the Play listing

LOW, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), disclosed as MEDIUM on 22 August 2026, reassessed in this report

The Data Safety card states that the app collects name, email address and user IDs and refers to the developer’s privacy policy. Neither the app page nor the Data Safety detail page exposes a link to an Ottobock-hosted policy. The only privacy-shaped link is Google’s generic policies.google.com/privacy. Direct requests to three likely Ottobock paths (/en/privacy-policy, /en-us/privacy, /en/data-protection) returned HTTP 404. A policy may exist at an address that was not guessed. CVSS does not score this transparency gap.

Source: Google Play listing and Data Safety page for com.ottobock.pro.connectgo, fetched on 22 August 2026. The privacy policy address is UNVERIFIED. A data subject looks first at the store listing, and a policy that cannot be reached from there is hard to find.

Impact: Clinicians who create an account cannot reach the notice that tells them what happens to their name, email address and user ID.

Fix: Link a privacy notice for this app in the Play listing and inside the app, and name a data protection officer in it.

M4: Patient configuration data is not represented in the Data Safety declaration

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B)

The Data Safety card lists name, email address and user IDs, which describe the clinician. The app's stated purpose is to read and write calibration, standard behaviour and My-Modes movement-pattern settings on a patient's prosthesis or orthosis. The patient is a second data subject who never installs the app and never sees its sign-in or consent screen. This report does not claim unlawful processing. Article 9(2)(h) is a plausible basis for a treating clinician configuring a prescribed device. The finding is that the public declaration does not reflect the second data subject. CVSS does not score it, so the severity is editorial. RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the undeclared data subject is a patient whose prosthesis configuration is health-related data, a context the CVSS technical scope does not capture.

The store description names the functions: standard behaviour setting for prostheses and orthoses, MyModes settings for special movement patterns and situations, calibration or static measurement and optimisation, and status information display.

The binary confirms a device command layer for these functions. The evidence is the capability interface Ottobock.Caa.Commanding.UOP.Core.UopDevice.Capabilities.ISliderRead and a literal Ottobock.Caa.ViennaRemoting.UNE.dll assembly name in the assembly store strings. The first notice cited Article 13(1). Because the patient does not supply the data personally, Article 14 is the information duty that applies to that data subject, and this report names it for completeness.

Impact: The people concerned are patients who wear microprocessor-controlled Ottobock prostheses and orthoses and whose gait-related settings are written through this app. They are not the app's users, so they have no screen on which to learn about the processing.

Fix: Describe the patient data category and its legal basis in the privacy notice and in the Data Safety declaration, and state a retention period for patient configuration data.

Impact Analysis

The app has two groups of people behind it. The clinicians who install it hold its accounts. The patients whose prostheses and orthoses are configured through it never see it. Those patients are people who wear a microprocessor-controlled leg component, and what the app writes decides how that component behaves.

This app is cleaner than the average of the programme, and this report says so. The findings are bounded. M1 concerns the strength of the sign-in channel, M2 a name inside the binary, M3 and M4 the transparency of the public declaration. The report does not claim any access to a patient's device and does not claim harm to any user.

The question that carries weight is not a numbered finding. It is whether authorisation is checked on the server for each configuration write and not only once at sign-in. The binary shows real identity federation and a single-use certificate concept, which is evidence against a purely client-side boundary, and it does not show that every write is re-checked.

The Complete Chain

Step	Evidence
A clinician signs in through Microsoft identity platform	MSAL redirect activity, AuthenticationActivity
A single-use qualification certificate is required to activate the professional role	localised strings in the assembly store
The app writes calibration and MyModes settings to the patient's device	store description, UopDevice capability interface, ViennaRemoting.UNE assembly name
The patient is a second data subject outside the app's consent screens	Data Safety card lists clinician data only
The app gates old versions through a bundled blocklist	version_blacklist.json
Whether each write is re-validated on the server	UNVERIFIED, requires dynamic and API-level testing

The chain is a chain of design questions and not an exploit path. Its last link can be answered by the manufacturer from its own design.

Version Blocklist as Remote-Configuration Capability

This is an observation without a severity.

```
{
  "Android_AppVersionCheck": {"> 0": {"blocked": ["< 1.5.2"]}},
  "Android_OsVersionCheck": {"> 0": {"blocked": ["< 12"]}},
  "iOS_AppVersionCheck": {"> 0": {"blocked": ["< 1.5.2"]}},
  "iOS_OsVersionCheck": {"> 0": {"blocked": ["< 15"]}}
}
```

The list shows that the app, or a remote counterpart of the same list, is designed to refuse operation on outdated app or OS versions. Whether enforcement happens only in the client, where it can be bypassed by anyone who can modify the app, or is checked again on the server before a configuration write is accepted was not verified. A version gate in a tool that writes to worn medical hardware reflects safety-engineering intent, and the open point is how strongly it is enforced.

Medical Device Context

The app's description places it in a clinical setting and the sibling notices on the Ottobock apps cite Annex I Section 17.2 of Regulation (EU) 2017/745 for software that controls a prosthesis. The first notice for this app did not cite an MDR article, and this report does not decide whether the app is a device or an accessory in the sense of the Regulation. The manufacturer can answer that. The question of server-side re-validation of every write is the one a cybersecurity risk file for such software would address.

Data Protection: Article by Article

Article	Relevance	Finding
9(2)(h)	Plausible basis for a treating clinician configuring a prescribed device	M4
13(1)	Accessible privacy information at the point of collection, completeness of the declared categories	M3, M4
14	Information duty for data not obtained from the data subject, relevant to the patient	M4
25	Staging artefacts in production, security by design	M1, M2
32(1)(b)	Integrity of the sign-in channel	M1
33(4)	Staged notification is expressly permitted if a breach is established	none

Regulatory & Legal Landscape

The bases are Regulation (EU) 2016/679 (GDPR) with Articles 9, 13, 14, 25, 32, 33 and 56, and for context Regulation (EU) 2017/745 Annex I Section 17.2. The disclosure follows ISO/IEC 29147 and rests on the freedom of research under Article 17 of the Austrian Staatsgrundgesetz.

The Datenschutzbehörde (dsb@dsb.gv.at) and the European Data Protection Supervisor (edps@edps.europa.eu) were in copy of the first notice. The publication date counts from delivery of the first notice.

Indicators of Compromise & Reproducible Evidence

Every item can be reproduced from the named package. No server was contacted other than the Google Play listing and three direct requests to ottobock.com paths for M3.

```
Package    com.ottobock.pro.connectgo 2.1.0 (95209)
Base APK   c67c3f3379f4faf777311f33cdab4522d919bb651dfd83837ecf96deecc9fc8f
XAPK       a00104ab0e17b23e153228698762f45ed284bcb5f82b8d703408080af0d17a67
Schemes    connectgopro, connectgopro-staging
Activity   crc648316b0a9aa8cfd61.BrowserTabActivity (exported)
Config     "GlamApi  and  "Host": "https://glam-api-sta  (truncated in the evidence)
Asset      assets/VersionCheck/version_blacklist.json
Store      lib/arm64-v8a/libassemblies.arm64-v8a.blob.so (80.3 MB, XABA v2)
Contacts   connectgo.pro@ottobock.com, apps@ottobock.com, myottobock@ottobock.com
Paths      /en/privacy-policy, /en-us/privacy, /en/data-protection on ottobock.com (
    HTTP 404)
```

Disclosure Timeline & Outcome

Date	Event
22 Aug 2026	First notice REF CONNECTGOPROBYOTTOBOCK-2026-R1 sent to connectgo.pro@ottobock.com, apps@ottobock.com and myottobock@ottobock.com, with the Datenschutzbehörde and the EDPS in copy. Three questions asked, written answer requested by 5 Sep 2026.
5 Sep 2026	Answer date requested in the first notice.
12 Sep 2026	Follow-up to the same three addresses with the questions repeated word for word, answer requested by 19 Sep 2026.
19 Sep 2026	Deadline set in the follow-up.
17 Oct 2026	Second follow-up with the unchanged questions and the 20 Nov 2026 embargo date.
15 Nov 2026	Final notice from s.kepp@rfi-irfos.com to the same three addresses (14:09 UTC), titled 5 days to publication, naming 20 Nov 2026 as the publication date.
20 Nov 2026	Publication date, 90 days after the first notice. Embargo date reached.
21 Nov 2026	Report published.

Outcome as of 21 November 2026: no substantive reply, no automatic acknowledgement and no bounce on any of the three addresses, including after the final notice of 15 November 2026.

What Ottobock Got Right

No hardcoded Firebase or Google API key and no secret-shaped token was found in the manifest, both dex files or the assembly store. No advertising, attribution or session-replay SDK is present, and no Chinese or sanctioned-jurisdiction SDK or endpoint. The set of dangerous permissions is minimal, with INTERNET, ACCESS_NETWORK_STATE, BLUETOOTH_CONNECT, BLUETOOTH_SCAN and VIBRATE only, and no location, camera, microphone, contacts or storage permission. BLUETOOTH_SCAN carries neverForLocation. allowBackup is false and extractNativeLibs is false. No custom network security configuration weakens the Android 15 default, so cleartext traffic is blocked. The only third-party SDK is New Relic Mobile, wrapped in Ottobock's own analytics assemblies.

The sign-in uses a real identity federation and a single-use professional qualification certificate. The localised text "Zertifikat bereits verwendet. Kontaktieren Sie Ihren Ottobock Trainer." shows the design intent, since a single-use certificate requires a shared state. The bundled version blocklist shows that outdated software is not meant to calibrate patient-worn hardware. These two points are the strongest evidence against a purely client-side boundary.

Residual Risk & Recommendations

Priority	Action	Finding
1	State in writing whether each configuration write is re-validated on the server	chain, M1
2	Confirm PKCE enforcement and remove the staging scheme from production	M1
3	Describe patient data and its legal basis in the privacy notice and the Data Safety declaration	M4
4	Publish an app-specific privacy notice and link it in the listing	M3
5	Remove staging configuration from the release build	M2

Residual risk: every copy of version 2.1.0 already distributed contains the staging scheme and the configuration fragment. This report describes version 2.1.0 only.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Root level code analysis of the published application plus the live Google Play listing. No Ottobock servers or accounts were probed and no device was paired. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Arts. 9, 13, 14, 25, 32, 33, 56. RFI-IRFOS ZVR 1015608684, GISA 39261441. REF CONNECTGOPROBYOTTOBOCK-2026-R1.