Security & Privacy Disclosure, Final Report

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

The patient app for Ottobock prosthetic knees carries the service, maintenance and test command library of the professional apps, and the one visible editability gate is a client-side integer.

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

Target	Otto Bock Healthcare Products GmbH, Vienna (group: Ottobock SE & Co. KGaA)
Versions Audited	1.0.0.227 / 164659 (analysis 2026-08-22)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days, unchanged)
Findings	6: 1 High, 3 Medium, 2 Low (C1 and C2 reassessed from Critical, H1 and H2 from High, M2 from Medium)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`d396c6b3eb961c538891f2a6b9ff5cc5367c980a88781ccc677bd61bcec91fb7`

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 5

4 Architecture & Data Flow 6

5 Findings 7
- 5.1 C1: Service, maintenance, test and file-transfer command library inside the patient app, parameter editing gated by a client-side integer . . . 7
- 5.2 C2: BLUETOOTH_PRIVILEGED declared in the manifest of a Play Store app . . 9
- 5.3 H1: The clinician app connectgo.pro stores local data without SQLCipher while connectgo and Cockpit encrypt it . . . 10
- 5.4 H2: "For qualified personnel" is listing text, and the patient and clinician apps share the same command vocabulary . . . 11
- 5.5 M1: No network security configuration and no certificate pinning . . . 12
- 5.6 M2: Two Microsoft Entra client IDs and enterprise broker queries in the manifest 13

6 Impact Analysis 13

7 The Complete Chain 14

8 Control and Remote-Configuration Data 14

9 Medical Device Context: MDR (EU) 2017/745 Annex I Section 17.2 15

10 Data Protection: Article by Article 15

11 Regulatory & Legal Landscape 16

12 Indicators of Compromise & Reproducible Evidence 16

13 Disclosure Timeline & Outcome 16

14 What Ottobock Got Right 17

15 Residual Risk & Recommendations 17

Executive Summary

connectgo is the patient-facing Bluetooth control app for Ottobock's microprocessor-controlled knees and orthoses, published by Otto Bock Healthcare Products GmbH in Vienna. On 22 August 2026 RFI-IRFOS sent six findings from a root level code analysis of version 1.0.0.227 under REF OTTOBOCKCONNECTGO-2026-R1. connectgo replaces the Cockpit app, and the clinician app connectgo.pro is its sibling.

The main finding concerns what the patient app contains. The binary holds fully implemented command classes for service, maintenance, test support, remote directory listing and file transfer on the paired device, and legacy commands that put the device to sleep, switch off its Bluetooth radio, make it beep and read its exception list. The only property found that decides whether an operating parameter can be edited is an integer named Permissions on the client model. The same command library is present in connectgo.pro and in Cockpit.

No device was paired and no command was sent. Whether the user interface reaches these commands, and whether the device firmware or the server checks authorisation independently of the client, are open questions that the manufacturer can answer. The other findings cover a declared system-level Bluetooth permission, a clinician app that stores local data without SQLCipher, a role separation that rests on listing text, missing certificate pinning and two Microsoft Entra client IDs.

Five of the six severities sent in the first notice are lowered in this report, because the evidence supports a lower band than the notice stated. 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 1.0.0.227 (versionCode 164659) as an XAPK: manifest and resources through apktool, targeted strings and symbol extraction on about 20 of 173 native libraries. 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
C1	HIGH	Service, maintenance, test and file-transfer command library inside the patient app, parameter editing gated by a client-side integer
C2	LOW	BLUETOOTH_PRIVILEGED declared in the manifest of a Play Store app
H1	MEDIUM	The clinician app connectgo.pro stores local data without SQLCipher while connectgo and Cockpit encrypt it
H2	MEDIUM	”For qualified personnel” is listing text, and the patient and clinician apps share the same command vocabulary
M1	MEDIUM	No network security configuration and no certificate pinning
M2	LOW	Two Microsoft Entra client IDs and enterprise broker queries in the manifest

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. Five of the six severities are lower here, because the evidence supports a lower band than the notice stated. Each finding states its reason.

ID	Sent 22 Aug 2026	This report	Basis
C1	CRITICAL	HIGH	CVSS 6.0, raised to HIGH for a load-bearing prosthesis, reason stated in the finding.
C2	CRITICAL	LOW	Declared permission, effect not shown. CVSS 0.0.
H1	HIGH	MEDIUM	Physical access needed, content of the database not examined. CVSS 4.1.
H2	HIGH	MEDIUM	Open architecture question, CVSS 0.0, editorial rating with reason.
M1	MEDIUM	MEDIUM	CVSS 6.3.
M2	MEDIUM	LOW	Public client IDs, transparency point. CVSS 0.0.

Subject & Operator Analysis

connectgo is the patient-facing Bluetooth control app for microprocessor-controlled Ottobock prosthetic knees and orthoses (C-Leg, Kenevo and the Genium family). It is published by Otto Bock Healthcare Products GmbH, Brehmstraße 16, 1110 Wien, Austria, telephone +43 1 523 37 86, the Austrian entity of Ottobock SE & Co. KGaA, Max-Näder-Straße 15, 37115 Duderstadt, Germany. The store listing describes it as the new and improved version of the Cockpit app. The store shows 500 plus installations and a PEGI 3 rating.

Item	Value
Package	com.ottobock.connectgo
Version	1.0.0.227 (versionCode 164659)
XAPK SHA-256	4cd7a92354afb4096d360ac2948228ee27a47f1b01beb4200a5ebbeed5e9fa89
Base APK SHA-256	d396c6b3eb961c538891f2a6b9ff5cc5367c980a88781ccc677bd61bcec91fb7
Size	189.4 MB bundle (base APK 17.7 MB, arm64-v8a native split 171.3 MB), arm64-v8a only
minSdk / targetSdk	31 / 36 (compileSdk 36)
Code base	.NET MAUI on Mono, 173 AOT assemblies (libaot-*.dll.so), two classes.dex files holding only the Java interop layer
Contact addresses (from the clinician sibling app)	connectgo.pro@ottobock.com, na.education@ottobock.com, ot-hotline@ottobock.de
Instructions for use	https://product-documents.ottobock.com/IFU/INT/560X34-1/647H1813/01/O/S/F
App-specific privacy policy	not found in the store listing or in the binary strings. Only the group policy https://corporate.ottobock.com/en/data-privacy-statement was located, and whether it covers connectgo is UNVERIFIED
Data protection officer	the group publishes a Global Data Privacy Officer contact form at https://corporate.ottobock.com/en/forms/gdpo-contact-form/. No direct address is published, and whether it applies to connectgo is UNVERIFIED

Supervisory competence: the manufacturer of record is Austrian, which supports the Datenschutzbehörde as first contact. If Ottobock SE & Co. KGaA in Duderstadt is the main establishment, the Niedersächsische Landesbeauftragte für den Datenschutz could be the lead authority. The question is raised and not settled here.

Architecture & Data Flow

connectgo carries the same device-communication framework as the clinician app connectgo.pro and the predecessor Cockpit. The framework is named Ottobock.Caa.* in the current apps and OBHC.CAA.* in the earlier ones, and the earlier name appears in Cockpit's own assemblies.manifest.

Layer	Observed	Source
Transport	Bluetooth LE GATT and Classic SPP with the TIO protocol	Caa.Bluetooth
Device commands	Protobuf-serialised command protocol and the legacy Vienna command set	Caa.Commanding, Caa.Commanding.UOP, Caa.ViennaRemoting. UNE
Device abstraction	Generic command queue for any command type	Caa.DeviceRemoting, BaseUopDevice queueing method
Integrity utilities	CRC8, CRC16 and CRC32	Caa.Checksum
Sign-in	Ottobock ID on Microsoft Entra ID through MSAL, two client IDs	AndroidManifest.xml
Local storage	SQLCipher	libe_sqlcipher.so
Telemetry	New Relic, in line with the app's own data safety statement of crash logs, diagnostics and other app performance data	libaot-NewRelic.* assemblies

The analysis used apktool on the base APK for manifest and resources and targeted strings and symbol extraction on about 20 priority native libraries out of 173. The full native split was not decompiled and no assembly store was parsed. Each finding states where this limits what can be said.

Findings

C1: Service, maintenance, test and file-transfer command library inside the patient app, parameter editing gated by a client-side integer

MEDIUM, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N, 6.0 (CVSS-B), editorial severity HIGH, disclosed as CRITICAL on 22 August 2026, re-assessed in this report

The patient-facing app contains fully implemented command classes for remote directory listing and file transfer on the paired prosthesis, binary dump reading, service and maintenance handling, a TestSupport command family and legacy device commands such as sleep mode, Bluetooth deactivation, beep and exception list. The one property found on the Slider data model that decides whether an operating parameter can be edited is a plain integer named Permissions, held on the client. A generic queueing method accepts any command type. Whether the shipped user interface reaches these commands, and whether the device firmware checks authorisation itself, were not tested. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.0 to HIGH because the commands act on a load-bearing prosthesis and the only visible gate is a client-held integer, a safety consequence that the CVSS technical scope does not capture.

```
Ottobock_Caa_Commanding_Service_ServiceDataBaseCommand__ctor
Ottobock_Caa_Commanding_Service_MaintenanceVariantBaseCommand__ctor
Ottobock_Caa_Commanding_Service_MaintenanceCondition_FromStream_System_IO_BinaryReader
Ottobock_Caa_Commanding_TestSupport_TestSupportBaseCommand__ctor
Ottobock_Caa_Commanding_TestSupport_LogData_FromStream_System_IO_BinaryReader
Ottobock_Caa_Commanding_FileTransfer_FileTransferBaseCommand__ctor
Ottobock_Caa_Commanding_FileTransfer_ListRemoteDirectoriesCommand_ReadDirectoryInfo_System_IO_Binary

    Reader
Ottobock_Caa_Commanding_FileTransfer_FileAppendSession_FileAppendSessionBaseCommand__ctor

Ottobock_Caa_Commanding_Dump_DumpBaseCommand__ctor
Ottobock_Caa_Commanding_Dump_DumpLineCommand__ctor
Ottobock_Caa_Commanding_Tube_TubeAdapterState_get_DriverEnabledAndRunning
Ottobock_Caa_Commanding_Tube_TubeAdapterState_get_ConfigurationInvalid

Ottobock_Caa_ViennaRemoting_UNE_Commands_ActivateSleepModeDeviceCommand__ctor_byte_System_Nullable_1

    _System_TimeSpan_System_Threading_CancellationToken
Ottobock_Caa_ViennaRemoting_UNE_Commands_DeactivateBluetoothDeviceCommand__ctor_System_Nullable_1_Sy

    stem_TimeSpan_System_Threading_CancellationToken
Ottobock_Caa_ViennaRemoting_UNE_Commands_BeepCommand__ctor_Ottobock_Caa_ViennaRemoting_UNE_Commands_


    BeepCommand_BeepType_System_Nullable_1_System_TimeSpan_System_Threading_CancellationToken

Ottobock_Caa_ViennaRemoting_UNE_Commands_GetExceptionListCommand__ctor
Ottobock_Caa_ViennaRemoting_UNE_Commands_CheckLastExceptionListCommand__ctor_byte___System_Nullable_

    1_System_TimeSpan_System_Threading_CancellationToken
Ottobock_Caa_ViennaRemoting_UNE_Commands_ConfigureDumpBytesDeviceCommand__ctor_System_Collections_Ge


    neric_IEnumerable_1_byte_System_Nullable_1_System_TimeSpan_System_Threading_CancellationToken

Ottobock_Caa_ViennaRemoting_UNE_Commands_AuthenticateDeviceCommand__ctor_string_byte___System_Nullab

    le_1_System_TimeSpan_System_Threading_CancellationToken_System_Action
Ottobock_Caa_ViennaRemoting_UNE_Commands_GetConfigurationByteCommand__ctor_string_byte___
    ...

Ottobock_Caa_Commanding_UOP_Core_Models_Slider_get_Permissions
Ottobock_Caa_Commanding_UOP_Core_Models_Slider_set_Permissions_int
Ottobock_Caa_Commanding_UOP_Core_Models_SliderExtensions_Validate_Ottobock_Caa_Commanding_UOP_Core_M

    odels_Slider_int
Ottobock_Caa_Commanding_UOP_Core_UopDevice_BaseUopDevice_QueueApplicationLayerCommandAsync_TApplicat

    ionLayerCommand_...
```

AOT-compiled .NET binaries keep the fully qualified method names as symbol names. The symbols above were read with strings on the native libraries. They show constructors, stream readers and validators, so the classes are implemented and not interface stubs. No decompiled logic was read.

Cross-app evidence: the same command assembly appears under its earlier name OBHC.

CAA.ViennaRemoting.UNE in the plaintext assemblies/assemblies.manifest of Cockpit. The command family has therefore been shipped in the consumer-facing app across at least two app generations.

Not tested: whether these commands are reachable from the shipped interface, whether the prosthesis firmware authorises a command beyond the AuthenticateDeviceCommand handshake and the client-held Permissions integer, and whether the CRC8, CRC16 and CRC32 utilities in Caa.Checksum protect authorisation or only transport integrity. No device was paired and no command was sent.

Impact: The people who rely on this app are users of microprocessor-controlled knees and orthoses (C-Leg, Kenevo and the Genium family). The app shipped to them contains the engineering and maintenance vocabulary of the device, and the gate on parameter editing that is visible in the client is one integer. A weakness here would reach the way a person's leg flexes and resists load while walking, which is the reason this report rates the finding above its technical score.

Fix: Remove service, maintenance and test command classes from the patient build. Enforce parameter-edit authorisation on the device firmware and on the server so that a client-side integer is never the deciding control. Document the authorisation model in writing.

C2: BLUETOOTH_PRIVILEGED declared in the manifest of a Play Store app

LOW, CVSS v4.0 AV:L/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 CRITICAL on 22 August 2026, reassessed in this report

The manifest declares android.permission.BLUETOOTH_PRIVILEGED. On stock Android this permission has the protection level signature or privileged and is reserved for platform apps and apps on an OEM allowlist, so an ordinary Play Store app does not obtain it through the permission dialog. The same declaration is in Cockpit and absent from connectgo.pro. It was not determined whether any device grants the permission to this app, so no effect is demonstrated and CVSS scores the finding at 0.0. It stays on the record as a question of data protection by design.

```
<uses-permission android:name="android.permission.BLUETOOTH"/>
<uses-permission android:name="android.permission.BLUETOOTH_PRIVILEGED"/>
<uses-permission android:name="android.permission.BLUETOOTH_CONNECT"/>
<uses-permission android:name="android.permission.BLUETOOTH_SCAN" android:
    usesPermissionFlags="neverForLocation"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
```

Two readings are possible. The declaration may be carried over from earlier code and have no effect on a normal device. Or the app may depend on an OEM allowlist for a capability such as pairing without a user-visible prompt. The evidence cannot tell the two apart. The legacy READ_EXTERNAL_STORAGE and WRITE_EXTERNAL_STORAGE permissions are also declared, which scoped storage on current Android has replaced.

Impact: A declared permission that the platform normally withholds from a store app does not harm a person by itself. For the users of connectgo the open point is whether the app needs, or silently relies on, a system-level Bluetooth capability that the standard Bluetooth permissions would not give it.

Fix: Remove the permission if it is unused, or document which capability needs it and on which devices it is granted.

H1: The clinician app connectgo.pro stores local data without SQLCipher while connectgo and Cockpit encrypt it

---

MEDIUM, CVSS v4.0 AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 4.1 (CVSS-B), disclosed as HIGH on 22 August 2026, reassessed in this report

The native library set of connectgo.pro contains libe_sqlite3.so and no SQLCipher provider. connectgo and Cockpit link SQLCipher. The result was cross-checked twice, in the native library listing and in the manifest.json split declaration of connectgo.pro. Which data the connectgo.pro database holds was not examined.

```
connectgo (patient, current): encrypted
  libe_sqlcipher.so
  libaot-SQLitePCLRaw.provider.e_sqlcipher.dll.so
Cockpit (patient, legacy): encrypted
  libsqlcipher.so (arm64-v8a and armeabi-v7a)
connectgo.pro (clinician): plain SQLite
  libe_sqlite3.so, no SQLCipher provider in the bundle
```

The clinician use case suggests that one device serves many patients, so a local cache on such a device would concentrate the data of many people. That is an inference from the purpose of the app. The content of the database was not read, and the exposure applies to a device that is lost, stolen or resold, or that is rooted.

Impact: Prosthesis and orthosis users whose configurations are handled by a clinic would be affected if a clinic device were lost or resold with a readable local database. The patient's own phone holds an encrypted database of only that person's data.

Fix: Move connectgo.pro to SQLCipher or an equivalent encrypted store, and document in a data protection impact assessment under Article 35 GDPR which patient data the clinician app caches.

H2: "For qualified personnel" is listing text, and the patient and clinician apps share the same command vocabulary

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), disclosed as HIGH on 22 August 2026, reassessed in this report

The note "For qualified personnel" on the connectgo.pro store page is description text. The only install-related check found is the generic com.android.vending.CHECK_LICENSE of Google Play, which is unrelated to professional credentials. Both apps sign users in through the same Ottobock ID system (Microsoft Entra ID through MSAL) and link the same Ottobock.Caa.Commanding and ViennaRemoting.UNE vocabulary. Whether the separation between patient and professional is enforced beyond the screens each app shows and a possible server-side role attribute was not determined. The finding is an open architecture question and CVSS does not score it. RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the unanswered question concerns who may change how a prosthesis behaves, a consequence the CVSS technical scope does not capture.

Property	connectgo (patient)	connectgo.pro (clinician)	Cockpit (legacy patient)
Runtime	.NET MAUI, per-assembly AOT, 173 libaot libraries	.NET MAUI or Xamarin, single blob libassemblies.arm64-v8a.blob.so, 80.3 MB, no AOT	Xamarin, assemblies.blob with plaintext assemblies.manifest
Local database	SQLCipher	plain SQLite	SQLCipher
BLUETOOTH_PRIVILEGED	declared	not declared	declared
READ and WRITE_EXTERNAL_STORAGE	declared	not declared	not checked
Shared Caa device stack	Ottobock.Caa.* (Bluetooth, Commanding, Commanding.UOP, DeviceRemoting, ViennaRemoting.UNE, DeviceManager, Checksum, Core)	Ottobock.Caa.* present in blob strings (for example Ottobock.Caa.ViennaRemoting.UNE.dll)	OBHC.CAA. ViennaRemoting.UNE and OBHC.CAA.Storage.Core (earlier namespace, in the manifest)
Play data safety	Personal info, app activity, health and fitness, app info and performance. No data shared with third parties.	Personal info only (name, email, user IDs). No data shared with third parties.	Personal info, health and fitness and two more. Shares app info and performance with third parties.
PEGI	3	3	3

Property	connectgo (patient)	connectgo.pro (clinician)	Cockpit (legacy patient)
Installs	500+	5,000+	100,000+

Any Play Store account can install connectgo.pro. The listing text of connectgo states that connectgo is the new and improved version of the Ottobock Cockpit app, the end-user app for Ottobock prostheses and orthoses.

Impact: Prosthesis users depend on the separation between the app a patient uses and the app a clinician uses. If the separation rests on the choice of app and not on a check that follows the user, the patient's own app is the weaker side of it.

Fix: State in writing where the separation between patient and professional roles is enforced, on the device, on the server or both, and add a server-side role check to every configuration write.

M1: No network security configuration and no certificate pinning

MEDIUM, CVSS v4.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B)

The manifest has no android:networkSecurityConfig attribute and res/xml has no network_security_config.xml. No usesCleartextTraffic override is declared. With targetSdkVersion 36 the platform default denies cleartext traffic, which mitigates the point. The absence of the file means no certificate pinning is configured for the backend used for account and activity-data sync.

The backend hostnames of connectgo were not extracted in this analysis, so the pinning question cannot be tied to named hosts.

Impact: Users who log in and sync activity data rely on the system trust store alone.

Fix: Add a network security configuration with certificate pinning for the account and sync hosts.

M2: Two Microsoft Entra client IDs and enterprise broker queries in the manifest

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 manifest embeds two MSAL redirect schemes with different client application IDs and declares queries for the Microsoft Authenticator and the Intune Company Portal. Client IDs are public identifiers and not secrets. The finding is a transparency point about why two exist and which processor sits behind sign-in. CVSS does not score it.

```
<data android:host="auth" android:scheme="msal92e27e5a-fc9a-47c8-a7d3-a8538414c4a0"/>
<data android:host="auth" android:scheme="msal9524e7f3-dc42-4fa1-9513-3a7a32fd11f5"/>
<package android:name="com.azure.authenticator"/>
<package android:name="com.microsoft.windowsintune.companyportal"/>
```

Client IDs: 92e27e5a-fc9a-47c8-a7d3-a8538414c4a0 and 9524e7f3-dc42-4fa1-9513-3a7a32fd11f5. The layout is consistent with Ottobock ID being built on a Microsoft Entra ID tenant. No store text or binary string found names Microsoft as a processor of sign-in data.

Impact: Users cannot see from the store disclosure which processor handles their sign-in.

Fix: Name the identity processor in the privacy notice and the data safety declaration and state what each client ID serves.

Impact Analysis

The people affected are wearers of Ottobock microprocessor-controlled knees and orthoses who use connectgo to control their device. The app is PEGI 3 rated and its store text calls it the end-user app.

The strongest point is C1. The patient build contains a command vocabulary written for service, maintenance, test and file access on the device, and the gate on editing a parameter that is visible in the client is a single integer. The consequence for a wearer would be a change to how the limb behaves, and for that reason the report rates the finding above its technical score. It does not claim that such a change is possible, because reachability and firmware checks were not tested.

H1 affects patients of clinics that use connectgo.pro. C2 and M2 are questions of design and transparency. No harm to any user is claimed by this report.

The Complete Chain

Step	Evidence
The public Play package contains the full Ottobock.Caa command library	libaot-Caa.Commanding*.dll.so, libaot-Caa.ViennaRemoting.UNE.dll.so
The library holds service, maintenance, test and file commands	symbol names quoted under C1
The only editability gate found is an integer on the client model	Slider.get_Permissions and set_Permissions
The same library exists in the clinician app and in Cockpit	native library listings, Cockpit assemblies.manifest
The clinician app is installable by any Play account	store listing and CHECK_LICENSE only
Both apps share the Ottobock ID sign-in	MSAL schemes in both manifests
Whether the device or the server re-checks authorisation	UNVERIFIED, depends on firmware and backend behaviour

The chain ends at an open question that the manufacturer can answer from its own design documents. That is the reason question 1 of the notice asks for the independent authorisation check.

Control and Remote-Configuration Data

The binary contains implemented commands that change the paired device's own state, among them ActivateSleepModeDeviceCommand, DeactivateBluetoothDeviceCommand and ConfigureDumpBytesDeviceCommand. A Dutch string found in the assembly blob of connectgo.pro says to check whether a software update for the component is possible, which indicates that the ecosystem supports software updates of the physical device.

This capability was not exercised. The remaining invisible-data categories were reviewed. Non-events need live pairing and are not evaluated. A household graph does not apply, because the app is built around one paired prosthesis per account. No notification-listener component exists. Bystander data has low relevance, because the activity data is generated by the wearer. The store already discloses fitness info and app interactions as collected categories.

Medical Device Context: MDR (EU) 2017/745 Annex I Section 17.2

The software controls a prosthetic knee and orthosis, so the manufacturer's obligations for medical device software are relevant. Annex I Section 17.2 of Regulation (EU) 2017/745 requires software in or as a device to be developed and manufactured according to the state of the art, taking into account the principles of the development life cycle, risk management including information security, and verification and validation.

The first notice did not assert a specific MDR article and this report does not decide whether connectgo is a device or an accessory in the sense of the Regulation, because that is for the manufacturer to state. The question of where authorisation is enforced for commands that reach a limb is the one an MDR risk file would answer.

Data Protection: Article by Article

Article	Relevance	Finding
5(1)(c)	Minimisation of declared permissions	C2
5(1)(f)	Integrity and confidentiality of the role separation	H2
13(1)(e)	Recipients and processors of sign-in data	M2
25	Design of command library, permission scope and role separation	C1, C2, H2
32(1)(a)	Encryption and transport protection	H1, M1
32(1)(b)	Integrity of processing systems with a physical effect	C1, H1, M1
33(4)	Staged notification is expressly permitted if a breach is established	none
35	Impact assessment for unencrypted multi-patient local storage	H1

Regulatory & Legal Landscape

The bases are Regulation (EU) 2016/679 (GDPR) with Articles 5, 13, 25, 32, 33 and 35, and 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 packages. No server was contacted and no device was paired.

```
Package     com.ottobock.connectgo 1.0.0.227 (164659)
XAPK        4cd7a92354afb4096d360ac2948228ee27a47f1b01beb4200a5ebbeed5e9fa89
Base APK    d396c6b3eb961c538891f2a6b9ff5cc5367c980a88781ccc677bd61bcec91fb7
Permission  android.permission.BLUETOOTH_PRIVILEGED
MSAL        msal92e27e5a-fc9a-47c8-a7d3-a8538414c4a0://auth
MSAL        msal9524e7f3-dc42-4fa1-9513-3a7a32fd11f5://auth
Queries     com.azure.authenticator, com.microsoft.windowsintune.companyportal
Property    Ottobock_Caa_Commanding_UOP_Core_Models_Slider_get_Permissions
Libraries   libaot-Caa.Commanding.dll.so, libaot-Caa.Commanding.UOP.dll.so, libaot-Caa
    .ViennaRemoting.UNE.dll.so, libaot-Caa.DeviceRemoting.dll.so
Sibling     com.ottobock.pro.connectgo base APK
    c67c3f3379f4faf777311f33cdab4522d919bb651dfd83837ecf96deecc9fc8f
Sibling     com.ottobock.prosthetics.ll.cockpit APK 17
    e203c1b57dac6a47098a9f2fe24cafbf72fe036ec51ffac6df5650fe7a09b2
```

Disclosure Timeline & Outcome

Date	Event
22 Aug 2026	First notice REF OTTOBOCKCONNECTGO-2026-R1 sent to info.austria@ottobock.com, myottobock@ottobock.com and connectgo.pro@ottobock.com, with the Datenschutzbehörde and the EDPS in copy. Sent the same day as the notices for Cockpit and connectgo.pro. Three questions asked.
12 Sep 2026	Follow-up to the same three addresses with the questions repeated word for word, answer requested by 26 Sep 2026.
26 Sep 2026	Deadline set in the follow-up.
17 Oct 2026	Second follow-up with the open findings and the unchanged questions.
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.

Date	Event
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

connectgo encrypts its local database with SQLCipher. The pairing and commissioning certificate mechanism appears to be taken seriously. Localised strings in connectgo.pro in at least five languages (Dutch, Norwegian, Swedish, Finnish, German) tell the user to contact an authorised Ottobock service centre or trainer when a pairing certificate has already been used. The Norwegian text reads "Sertifikat allerede brukt. Kontakt Ottobock-treneren din." This is consistent with a design in which a consumed credential cannot simply be reset by the end user. The cryptographic strength of the scheme was not examined.

No hardcoded Firebase or Google API key and no secret-shaped token was found in the extracted resources or libraries. No advertising, session-replay or China-jurisdiction SDK is present, and the only third-party telemetry is New Relic, which matches the app's own data safety statement. targetSdkVersion 36 denies cleartext traffic by default, android:allowBackup is set to false, and CRC8, CRC16 and CRC32 utilities exist for transfer integrity.

Residual Risk & Recommendations

Priority	Action	Finding
1	Document where parameter-edit authorisation is enforced and remove service, maintenance and test commands from the patient build	C1
2	State where the patient and professional separation is enforced	H2
3	Encrypt the connectgo.pro local database and complete a data protection impact assessment	H1
4	Document or remove BLUETOOTH_PRIVILEGED and the legacy storage permissions	C2
5	Pin certificates for account and sync hosts	M1
6	Name the identity processor and publish an app-specific privacy notice	M2

Residual risk: every copy of version 1.0.0.227 already distributed contains the command library. This report describes version 1.0.0.227 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.

No Ottobock servers or accounts were probed and no device was paired. ISO/IEC 29147, Art. 17 StGG, GDPR Arts. 5, 13, 25, 32, 33, 35, MDR (EU) 2017/745 Annex I Section 17.2. RFI-IRFOS ZVR 1015608684, GISA 39261441. REF OTTOBOCKCONNECTGO-2026-R1.