Security & Privacy Disclosure, Final Report

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

The control app for Ottobock's myoelectric hands and arms carries bootloader, update and permission-write commands in the one build that every patient installs.

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	1.0.53 / 53 (analysis 2026-08-22)
Notice / Publication	2026-08-22 / 2026-11-20 (90 days, unchanged)
Findings	6: 1 High, 3 Medium, 2 Low (C1 reassessed from Critical, H1, H2 and H3 from High, M2 from Medium)
Status	NO SUBSTANTIVE REPLY AS OF 21 NOVEMBER 2026
SHA-256 (base APK)	`e1dbde1d57e528bd38b897c5e60c37da016869b47a4a948ee51cdd2baa9cc8c3`

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 Shared Platform Across Four Apps and Two Product Lines 7

6 Findings 8

6.1 C1: Bootloader, update, file-transfer and permission-write commands inside the single app that patients and clinicians both install . . . 8

6.2 H1: The app's privacy notice calls MAC address, Bluetooth ID and article number anonymised, and the Play Data Safety card omits device identifiers 10

6.3 H2: Myoelectric signal recording and the building of a personal motion classifier are not named in the privacy notice . . . 11

6.4 H3: Custom-scheme OAuth redirect on an exported activity, and an authentication stack that differs from the sibling apps . . . 12

6.5 M1: No network security configuration and no certificate pinning . . . 13

6.6 M2: A New Relic handler wraps all outbound HTTP calls, and New Relic is not named in the privacy notice . . . 13

7 Impact Analysis 14

8 The Complete Chain 14

9 Inference Data and Control Data 15

10 Release Note Artefact 15

11 Medical Device Context 15

12 Data Protection: Article by Article 16

13 Regulatory & Legal Landscape 16

14 Indicators of Compromise & Reproducible Evidence 17

15 Disclosure Timeline & Outcome 17

16 What Ottobock Got Right 18

17 Residual Risk & Recommendations 18

Executive Summary

connectgrip. by ottobock. is the control app for Ottobock's myoelectric hand and arm prostheses, published by Otto Bock Healthcare Products GmbH in Vienna with more than 500 installations on Google Play. On 22 August 2026 RFI-IRFOS sent six findings from a root level code analysis of version 1.0.53 under REF OTTOBOCKCONNECTGRIP-2026-R1. It was the fourth and last part of a family comparison with Cockpit, connectgo.pro and connectgo.

The main finding concerns what the single, combined patient and clinician app contains. The binary holds fully implemented commands to put the connected prosthesis into bootloader mode, to load and apply a firmware update bundle, to store, append, retrieve, erase and list files on the device, and to write the permission that decides whether a parameter can be edited. The same Ottobock.Caa device platform exists in the knee apps, and connectgrip is the first app in which it serves a different product line. No device was paired and no command was sent. Whether the interface reaches these commands and whether the device firmware or the server checks authorisation independently are open questions that the manufacturer can answer.

Two findings concern what users are told. The app's privacy notice calls the MAC address, Bluetooth ID and article number of the control unit anonymised while the Play Data Safety card lists no device identifiers, and the app records a user's muscle signals and builds a personal classifier from them without naming this anywhere in the notice. Further findings cover a custom-scheme sign-in redirect, missing certificate pinning and an analytics handler on all HTTP calls.

Five of the six 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 1.0.53 (versionCode 53) as an XAPK obtained through a mirror and cross-checked against the live listing: manifest and resources through apktool, targeted strings and symbol extraction on 17 of 203 native libraries, and the bundled privacy notice and terms. 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	Bootloader, update, file-transfer and permission-write commands inside the single app that patients and clinicians both install
H1	MEDIUM	The app's privacy notice calls MAC address, Bluetooth ID and article number anonymised, and the Play Data Safety card omits device identifiers
H2	MEDIUM	Myoelectric signal recording and the building of a personal motion classifier are not named in the privacy notice
H3	LOW	Custom-scheme OAuth redirect on an exported activity, and an authentication stack that differs from the sibling apps
M1	MEDIUM	No network security configuration and no certificate pinning
M2	LOW	A New Relic handler wraps all outbound HTTP calls, and New Relic is not named in the privacy notice

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 6.1, raised to HIGH for a device that moves a person's hand, reason stated in the finding.
H1	HIGH	MEDIUM	Editorial rating, CVSS 0.0, reason stated in the finding.
H2	HIGH	MEDIUM	Editorial rating, CVSS 0.0, local processing, reason stated in the finding.
H3	HIGH	LOW	Likely PKCE mitigation, CVSS 1.8, same pattern as connectgo.pro.
M1	MEDIUM	MEDIUM	CVSS 6.3.
M2	MEDIUM	LOW	Capability without a captured data flow, CVSS 0.0.

Subject & Operator Analysis

connectgrip. by ottobock. is the control app for Ottobock's myoelectric upper-limb prostheses, hands and arms (bebionic, myosmart, myosmart plus, myosmart cuff and related terminal devices). Unlike the lower-limb family, there is one combined app for qualified personnel and users. Patients and clinicians install the same binary, and a linked MyOttobock Pro account is the only distinction. The developer on Google Play is Ottobock SE & Co. KGaA. The controller named in the app's own privacy notice is Otto Bock Healthcare Products GmbH, Brehmstraße 16, 1110 Wien, Austria, represented by Dr Andreas Eichler, FN 242378 p, Handelsgericht Wien, telephone +43 1 523 37 86, fax +43 1 523 22 64. The store shows 500 plus installations and an all-ages rating (Everyone in the US listing, USK 0 in the German listing).

Item	Value
Package	com.ottobock.connectgrip
Version	1.0.53 (versionCode 53)
XAPK SHA-256	2c7dd2c5b431d95bf84cb033c7e7757d2b53f938cc729fe3b522f3c873000524 (179,629,861 bytes)
Base APK SHA-256	e1dbde1d57e528bd38b897c5e60c37da016869b47a4a948ee51cdd2baa9cc8c3 (95,376,236 bytes)
Native split SHA-256	a4f8d4d3a3b98b64fca7c32978343a0a003b0997a526f17454120d6fd911687e (config.arm64_v8a.apk, 81,964,574 bytes)
minSdk / targetSdk	31 / 34 (compileSdk 34)
Code base	.NET MAUI on Mono, 203 AOT assemblies (libaot-*.dll.so), arm64-v8a only, two classes.dex files holding only the Java interop layer
Source of the package	APKPure mirror. Package, developer and version were cross-checked against the live Google Play listing in the en-US and de-DE variants before and after the download. The mirror's binary carries a last-modified date of 14 April 2026 and the live listing shows Updated on Jun 18, 2026. versionCode 53 is the only version in the mirror's history
Privacy contacts (from the app's own notice)	apps.austria@ottobock.com, NAPrivacy@ottobock.com (US and Canada), Global Data Privacy Office form at https://corporate.ottobock.com/de/contact-gdpo
Support address (Play listing)	connectgrip@ottobock.com
Referenced MyOttobock Pro policy	https://my.ottobock.com/legal?id=PN_MyOB_Pro&lng=de, reachability from outside an authenticated session is UNVERIFIED
Instructions for use	https://product-documents.ottobock.com/IFU/INT/13E522/647G1837/01/O/S/F

A sibling package com.ottobock.connectgripna (connectgrip. by ottobock NA) exists on

Google Play and was not audited. Supervisory competence: the controller of record is Austrian, which supports the Datenschutzbehörde as first contact. Ottobock SE & Co. KGaA in Duderstadt is named in the notice as the separate controller for MyOttobock and MyOttobock Pro account processing, and the Niedersächsische Landesbeauftragte für den Datenschutz could be the lead authority for that component. The question is raised and not settled here.

Architecture & Data Flow

The application logic is AOT-compiled .NET. The analysis used apktool on the base APK for manifest and resources and targeted strings and symbol extraction on 17 priority native libraries out of 203. The full native split was not decompiled. Findings rest on string and symbol evidence.

Layer	Observed	Source
Transport	Ottobock.Caa.Bluetooth with the TIO protocol classes	libaot-Bluetooth.dll.so
Device remoting	Vienna protocol and SimpleAuthenticator pairing authentication with a failure counter	libaot-DeviceRemoting.dll.so
Command layer	Caa.Commanding including BootLoader, RemoteUpdate, FileTransfer, Dump, TestSupport, Slider and Radio families	libaot-Commanding.dll.so
Product layer	AxonNxt.Commanding and AxonNxt.Driver for hand, elbow, thumb sensor, glove mode, classifier, rotator, motion, file transfer, signal, factory reset, software reset, deep sleep and switching events	libaot-AxonNxt.*.dll.so
Recording	Pattern-recognition recording and classifier building	libaot-AxonNxt.App.Core.dll.so
Sign-in	WebAuthenticator with IdentityModel.OidcClient, custom scheme axonnxtapp	AndroidManifest.xml
Local storage	SQLCipher	libe_sqlcipher.so
Telemetry	New Relic through ObAnalytics.Maui, HTTP handler and navigation tracking	libaot-ObAnalytics.Maui.dll.so

Shared Platform Across Four Apps and Two Product Lines

The same Ottobock.Caa device platform appears in four independently downloaded Play Store apps. connectgrip is the first member that belongs to a different prosthesis product line.

App	Package	Product line	Shared evidence
connectgo	com.ottobock.connectgo	Lower limb (C-Leg, Genium, Kenevo)	Caa.Bluetooth (TIO), Caa.Commanding, Commanding.UOP, ViennaRemoting.UNE, DeviceRemoting
connectgo.pro	com.ottobock.pro.connectgo	Lower limb, clinician	Ottobock.Caa.ViennaRemoting.UNE.dll, UopDevice (assembly store strings)
Cockpit	com.ottobock.prosthetics.ll.cockpit	Lower limb, legacy	OBHC.CAA.ViennaRemoting.UNE (earlier name, plaintext manifest)
connectgrip	com.ottobock.connectgrip	Upper limb (bebionic, myosmart)	Caa.Bluetooth.TIO, Caa.Commanding, ViennaProtocol, SimpleAuthenticator, CaaChecksum

The product wrappers differ. Caa.Commanding serves the knee line and AxonNxt.Commanding serves the hand and arm line. AxonNxt.Commanding and AxonNxt.Driver are built directly on the shared ApplicationLayerCommand, IBluetoothManager and IBluetoothAdapterService abstractions. This is a finding about architecture and namespace identity. It does not claim that any specific vulnerability chain reaches across all four apps, and the reachability and firmware-side authorisation of commands remain open per app.

The practical consequence is that a defect class in the shared DeviceRemoting or Bluetooth layer, for example the SimpleAuthenticator byte-key pairing or the TIO advertisement parser, is a question for Ottobock’s Bluetooth-connected portfolio as a whole and not for one app.

Findings

C1: Bootloader, update, file-transfer and permission-write commands inside the single app that patients and clinicians both install

MEDIUM, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N, 6.1 (CVSS-B), editorial severity HIGH, disclosed as CRITICAL on 22 August 2026, re-assessed in this report

The binary contains fully implemented command classes for entering the bootloader of the connected prosthesis (JumpToBootLoaderCommand), loading and applying a firmware update bundle, storing, appending, retrieving, erasing and listing files on the device, reading raw dumps, a TestSupport family, and a Slider family in which WriteSliderPermissionCommand is an outbound command that carries a slider index and a permission value. The device service surface includes factory reset, software reset and deep sleep mode. connectgrip has no separate clinician build, so this vocabulary is in the one binary every user installs. Whether the user interface reaches these commands, and whether the device firmware checks authorisation beyond the SimpleAuthenticator byte-key handshake, were not tested. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.1 to HIGH because the commands include bootloader entry and a permission write aimed at a device that actuates grip force next to a person’s body, a safety consequence that the CVSS technical scope does not capture.

```
Ottobock_Caa_Commanding_BootLoader_JumpToBootLoaderCommand_get_UpdateType
Ottobock_Caa_Commanding_RemoteUpdate_LoadBundleCommand_get_FilePath
Ottobock_Caa_Commanding_RemoteUpdate_ConditionalEnterRemoteUpdateCommand_set_ProhibitedByApplication

    Reason_byte

Ottobock_Caa_Commanding_FileTransfer_StoreFileOnRemoteHostCommand_get_Data
Ottobock_Caa_Commanding_FileTransfer_AppendDataToRemoteFileCommand_get_Data
Ottobock_Caa_Commanding_FileTransfer_EraseRemoteFileCommand_get_Id
Ottobock_Caa_Commanding_FileTransfer_RetrieveRemoteFileCommand_get_Id
Ottobock_Caa_Commanding_FileTransfer_ListRemoteFilesCommand_get_NumberOfFiles
Ottobock_Caa_Commanding_FileTransfer_GetAvailableMemorySpaceCommand_set_AvailableMemorySpace_uint


Ottobock_Caa_Commanding_Dump_StartDumpCommand_get_DumpTargetNode
Ottobock_Caa_Commanding_Dump_ConfigureDumpCommand_get_DumpValueIds
Ottobock_Caa_Commanding_Dump_GetDetailedDumpInformationCommand_get_DumpValueDescriptions


Ottobock_Caa_Commanding_TestSupport_TestSupportBaseCommand__ctor
Ottobock_Caa_Commanding_TestSupport_LogData_FromStream_System_IO_BinaryReader
Ottobock_Caa_Commanding_TestSupport_DetailedLogData_set_EventData_byte__

Ottobock_Caa_Commanding_Slider_WriteSliderPermissionCommand_get_SliderIndex
Ottobock_Caa_Commanding_Slider_WriteSliderPermissionCommand_get_Permission
Ottobock_Caa_Commanding_Slider_WriteSliderUserValueCommand_get_Value
Ottobock_Caa_Commanding_Slider_WriteSliderValueCommand_get_Value

Ottobock_Caa_Commanding_Radio_SetBluetoothModulePowerCommand_set_BluetoothPowerState_Ottobock_Caa_Co

    mmanding_Radio_PowerState

AxonNxt_Commanding_Helper_ApplicationLayerCommandExtensions_ParsingException_Ottobock_Caa_DeviceRemo

    ting_UnifiedCommanding_ApplicationLayer_ApplicationLayerCommand
AxonNxt_Driver_NxtDriver__ctor_AxonNxt_Driver_Abstractions_Contracts_INxtUnifiedApplicationDevice_st

    ring_Ottobock_Caa_Bluetooth_IBluetoothManager_...
AxonNxt_Driver_NxtDevice__ctor_Ottobock_Caa_Bluetooth_IBluetoothAdapterService_...
    _Abstractions_Cont
    racts_IFactoryResetService_..._ISoftwareResetService_..._IDeepSleepModeService_...
```

AOT-compiled .NET binaries keep fully qualified method names as symbol names. The names above show constructors and property accessors, so the classes are implemented and not interface stubs. No decompiled logic was read.

Shared platform: the handler ApplicationLayerCommandExtensions.ParsingException in AxonNxt.Commanding is declared on Ottobock.Caa.DeviceRemoting.UnifiedCommanding.ApplicationLayer.ApplicationLayerCommand, the base abstraction under the command set of the knee app connectgo. The Ottobock.Caa.Bluetooth.TIO classes (TioAdvertisement, TioDataSource, BleScanRecord.HandleManufacturerSpecificData) are the same BLE transport family that connectgo uses. Ottobock.Caa.DeviceRemoting.ViennaRemoting.ViennaProtocol and Ottobock.Caa.DeviceRemoting.Authentication.SimpleAuthenticator with SimpleAuthenticationCommand (a byte-array key and a FailedSimpleAuthentications counter) match the Vienna remoting classes that appear as OBHC.CAA.ViennaRemoting.UNE in the plaintext assembly manifest of Cockpit.

Not tested: reachability of JumpToBootLoaderCommand, the file-transfer commands and WriteSliderPermissionCommand from the shipped interface, independent firmware validation of a permission write or a bootloader request, and what SetBluetoothModulePowerCommand and the deep sleep service are gated by. No device was paired and no command was sent.

Impact: The people who rely on this app wear a myoelectric hand or arm prosthesis (bebionic, myosmart, myosmart plus and related terminal devices). The device actuates grip force next to the wearer's body. The app they install contains the command to put that device into firmware-flashing mode and a command to write the permission that decides whether a parameter can be edited. A weakness in this surface would reach a device that moves a person's hand, which is the reason this report rates the finding above its technical score.

Fix: Remove bootloader, update, file-transfer and test commands from the build that patients install, or gate them on the device and on the server with authenticated authorisation. Document the authorisation model for permission writes in writing.

H1: The app's privacy notice calls MAC address, Bluetooth ID and article number anonymised, and the Play Data Safety card omits device identifiers

---

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 bundled privacy notice (assets/dpn/dpn_en.htm, last updated 2025-01-16) says that the app receives anonymised information about its use and that technical data of the control unit (MAC address, Bluetooth ID and article number) may be processed, also for a personal user without a linked MyOttobock account. The live Play Data Safety card lists name, email address and user IDs and no device or other IDs. The two disclosure surfaces are controlled by the same operator and differ. CVSS does not score this transparency finding, so the severity is editorial. RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the two disclosure surfaces belong to the same operator and the identifier belongs to a medical device worn by the user, a context the CVSS technical scope does not capture.

Verbatim from the privacy notice: "If you use the connectgrip app as a personal user without linking to your MyOttobock account, no personal data will be transmitted in general. However, we receive anonymised information about the use of the app, including error information. For this purpose, technical data of your device (software version, device settings, model, status, usage and error information) as well as technical data of the control unit (MAC address, Bluetooth ID and article number) may be processed."

Verbatim from the Data Safety card, fetched on 22 August 2026: "This app may collect these data types: Personal info. Name, Email address, and User IDs." No Device or other IDs category appears.

A Bluetooth MAC address and a device-specific Bluetooth ID are widely treated as identifiers that can relate to a natural person under Article 4(1) and Recital 30 GDPR when a controller can link them, for example to a MyOttobock account, a support case or a repeat connection pattern. This report finds the label anonymised hard to reconcile with the technical facts named in the same paragraph. It does not decide the question. It asks for the basis.

Impact: Users of a myoelectric prosthesis read two different statements about what the app collects, and neither tells them clearly that a device identifier of their prosthesis is processed.

Fix: Align the Data Safety declaration with the privacy notice, declare device identifiers, and justify or drop the label anonymised for identifiers that can be linked.

H2: Myoelectric signal recording and the building of a personal motion classifier are not named in the privacy notice

---

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 binary contains a fully implemented feature that records the user's own myoelectric pattern-recognition samples (StartPatternRecognitionRecordingAsync, FeatureRecording.Recording with a RecordingDuration), tags them with AmputationSide and ProsthesisHandType, and builds a personal classifier from them (BuildClassifierService, Classifier, IndividualClassifier). The complete bundled privacy notice contains no occurrence of recording, signal, classifier, muscle, EMG, myoelectric or biometric. The notice states that product data stays on the mobile device, and this report does not claim that the recordings leave it. CVSS does not score the gap, so the severity is editorial. RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because the unnamed processing concerns neuromuscular signals tied to a typed amputation side of the user, health-related data that the CVSS technical scope does not capture.

```
AxonNxt_App_Core_ViewModels_ManageRecordingsBaseViewModel_StartPatternRecognitionRecordingAsync_
    ...
AxonNxt_App_Core_Services_BuildClassifierService_BuildClassifierIfNeededAsync_AxonNxt_Driver_Abstrac

    tions_Models_Classifier_string
AxonNxt_App_Core_ViewModels_BasicControl_ManageBasicControlRecordingsPageViewModel_AddRecordingsForM

    otionType_..._AmputationSide_ProsthesisHandType_byte
AxonNxt_App_Core_ViewModels_Documentation_DocumentationPageViewModel_set_AmputationSide_AxonNxt_Driv

    er_Abstractions_Constants_AmputationSide
AxonNxt_App_Core_ViewModels_EvaluationPageViewModel_set_AmputationSide_AxonNxt_Driver_Abstractions_C

    onstants_AmputationSide
AxonNxt_Driver_Abstractions_Models_FeatureRecording_Recording_get_RecordingDuration
AxonNxt_Driver_Abstractions_Models_Classifier__ctor_System_Collections_Generic_IEnumerable_1_AxonNxt

    _Driver_Abstractions_Models_FeatureRecording_Recording
AxonNxt_Driver_Abstractions_Models_IndividualClassifier__ctor_System_Collections_Generic_IEnumerable

    _1_AxonNxt_Driver_Abstractions_Models_FeatureRecording_Recording
```

This is the mechanism by which a user trains the prosthesis to recognise the patterns of their own residual-limb muscle signals, consistent with the store description of recording individual movements to compensate for unwanted behaviours. The privacy notice describes only account data (name, email, country, MyOttobock authorisations) and generic product data (model, serial number, software version, settings, status, service information).

Article 4(2) GDPR defines processing to include automated operations on data whether or not it leaves the device, so building a classifier from a user's recordings is processing. Neuromuscular signal data tied to an amputation plausibly falls within data concerning health under Article 9(1). This report does not assert that the data is biometric data used to identify

a person, because the classifier identifies an intended motion and not the person. A feature this central to the app's purpose that appears nowhere in the notice is an Article 13(1) completeness gap wherever the resulting data is stored.

Impact: The people affected are wearers of myoelectric hands and arms who record their own muscle signals in the app. They are told about their account data and product data and not about the recording and the personal model that the app builds from it.

Fix: Name the recording and classifier feature, its purposes, its legal basis under Article 9(2) and where the data is stored in the privacy notice.

H3: Custom-scheme OAuth redirect on an exported activity, and an authentication stack that differs from the sibling apps

---

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 HIGH on 22 August 2026, reassessed in this report

The exported AuthenticationCallbackActivity catches the custom scheme axonnxtapp. The app uses .NET MAUI WebAuthenticator with IdentityModel.OidcClient, not the MSAL library of connectgo. A custom scheme is not exclusively claimable, so another app could register the same scheme and receive the redirect. IdentityModel.OidcClient supports PKCE and current versions enable it by default. Whether PKCE is enforced end to end was not verified, and the score assumes that it is.

```
<activity android:exported="true" android:launchMode="singleTop"
    android:name="crc64b0a56c7316c353e7.AuthenticationCallbackActivity" android:
    noHistory="true">
    <intent-filter>
        <action android:name="android.intent.action.VIEW"/>
        <category android:name="android.intent.category.DEFAULT"/>
        <category android:name="android.intent.category.BROWSABLE"/>
        <data android:scheme="axonnxtapp"/>
    </intent-filter>
</activity>
<activity android:exported="false" android:name="crc6468b6408a11370c2f.
    WebAuthenticatorIntermediateActivity"/>
```

The native library set holds libaot-IdentityModel.dll.so, libaot-IdentityModel.OidcClient.dll.so and the JWT token stack, and no Microsoft.Identity.Client library. The manifest declares no msal scheme and no queries for the Microsoft Authenticator or the Intune Company Portal, all of which connectgo declares. The privacy notice says clinicians sign in with a MyOttobock Pro account used for verification in the sense of a single sign-on.

Two different OAuth client implementations against what the operator describes as one account system also split security review, because a flaw class fixed in one implementation is not fixed in the other. The clinician app connectgo.pro ships a comparable custom-scheme redirect with the schemes connectgopro and connectgopro-staging.

Impact: Clinicians who sign in with a MyOttobock Pro account on this app would be the users affected, and through them the patients whose devices they configure.

Fix: Confirm PKCE enforcement for the redirect flow and consider claimed HTTPS redirects. Align the sign-in implementation across the Ottobock apps.

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 cleartext override is declared. With targetSdkVersion 34 the platform default denies cleartext traffic, which mitigates the point. No certificate pinning exists for the backend that the account and telemetry paths use.

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

Impact: Users who sign in and send telemetry rely on the system trust store alone.

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

M2: A New Relic handler wraps all outbound HTTP calls, and New Relic is not named in the privacy notice

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

Ottobock's own ObAnalytics.Maui library installs a NewRelicHttpClientHandler on the HTTP pipeline, so request URL, response code and timing can be passed to the New Relic NoticeHttpTransaction API, in addition to navigation tracking and exception reporting. This is a capability and not a demonstrated data flow, because no traffic was captured. The privacy notice refers only to error information and does not name New Relic as a recipient. CVSS does not score it.

```
ObAnalytics_Maui_Targets_NewRelicPlugin_NewRelicHttpClientHandler__ctor
ObAnalytics_Maui_Targets_NewRelicPlugin_NewRelicHttpClientHandler__n__0_System_Net_Http_HttpRequestM

    essage_System_Threading_CancellationToken
Com_Newrelic_Agent_Android_NewRelic_NoticeHttpTransaction_string_string_int_long_long_long_long_stri

    ng_...
Com_Newrelic_Agent_Android_NewRelic_NoticeDistributedTrace_System_Collections_Generic_IDictionary_2_

    string_string
ObAnalytics_Maui_Targets_NewRelicTarget_RecordNavigation_string_string_string_string
```

Because the handler sits at the transport layer, any backend request URL or header that carries an identifier such as an account number, device serial or MAC-derived value would be visible to the instrumentation by construction. New Relic is a US-based processor. The mechanism for a third-country transfer is not addressed in the reviewed notice.

Impact: Users cannot see from the notice which processor receives technical data about the app's network use.

Fix: Name the analytics processor and the transfer mechanism in the privacy notice, and

scope the HTTP instrumentation so that URLs and headers with identifiers are excluded.

Impact Analysis

The people affected wear myoelectric hands and arms from Ottobock and use connectgrip to control them. Many are adults with an acquired upper-limb amputation. The store rates the app for all ages, while the app records a user's muscle signals and handles a typed amputation side.

The strongest point is C1. The only build available to patients contains the command to put the connected device into firmware-flashing mode, a file system on the device and a command that writes the permission deciding whether a parameter can be edited. The consequence for a wearer would be a change to how the hand or arm behaves. The report does not claim that such a change is possible, because reachability and firmware checks were not tested.

H1 and H2 concern what users are told. They read two different statements about identifiers and no statement about the recording of their muscle signals. H3 and M2 are bounded questions on the sign-in channel and on analytics. No harm to any user is claimed by this report.

The Complete Chain

Step	Evidence
There is one app for patients and clinicians	store listing and bundled privacy notice, no separate pro build
The app carries the full Ottobock.Caa command library	libaot-Commanding.dll.so, libaot-DeviceRemoting.dll.so
The library holds bootloader entry, update bundle, file transfer and permission write	symbol names quoted under C1
The pairing step is a byte-key SimpleAuthenticator	libaot-DeviceRemoting.dll.so
The same platform exists in four apps and two product lines	table above
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. That is the reason question 1 of the notice asks for the independent authorisation check.

Inference Data and Control Data

The locally built classifier is a derived model that ties more directly to a user's neuromuscular state than any single raw value. It is not named as a processing category in the notice (H2).

The control capabilities are JumpToBootLoaderCommand, RemoteUpdate. LoadBundleCommand, ConditionalEnterRemoteUpdateCommand, SetBluetoothModule-PowerCommand and the deep sleep, factory reset and software reset services. They change the paired device's own operational state, including entry into a firmware-flashing mode. None of this was exercised.

Bystander data applies when a clinician operates the app on a patient's device. The notice states that product data (model, serial number, software version, settings, status, service information) is processed and stored only on the mobile device and that the manufacturer has no access to these locally stored data. That statement is specific and is not contradicted by anything found, and it was not checked against network traffic. Non-events were not evaluated. A household graph and notification mirroring do not apply.

Release Note Artefact

This is an observation without a severity.

```
assets/release.txt
Merged PR 10947: NXTA-2803: Prevent double control activation
```

The line is the app's own change reference for the shipped build. It documents a fix for a double control activation condition, which suggests that the control layer has had at least one defect related to unintended repeat activation of a control function. The underlying ticket was not available, and this report does not assert what the condition affected.

Medical Device Context

The app controls a prosthetic hand or arm, 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 for this app did not cite an MDR article, and this report does not decide whether connectgrip is a device or an accessory in the sense of the Regulation. The manufacturer can answer that. The question of independent authorisation for bootloader entry and permission writes is the one an MDR cybersecurity risk file would address.

Data Protection: Article by Article

Article	Relevance	Finding
4(1), Recital 30	Device identifiers as online identifiers	H1
4(2)	On-device recording and classifier building is processing	H2
5(1)(a)	Transparency of the two disclosure surfaces	H1, H2
9(1), 9(2)	Neuromuscular signals and amputation side as data concerning health, legal basis not stated	H2
13(1)(c)	Purposes of processing must be stated	H2
13(1)(e)	Recipients of technical data	M2
25	Command library scope and authentication tooling	C1, H3
32(1)(a), (b)	Integrity of processing systems, transport and sign-in channel	C1, H3, M1
44	Third-country transfer to a US analytics processor, mechanism not stated	M2

Regulatory & Legal Landscape

The bases are Regulation (EU) 2016/679 (GDPR) with Articles 4, 5, 9, 13, 25, 32 and 44, 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 Ottobock server was contacted and no device was paired.

```
Package    com.ottobock.connectgrip 1.0.53 (53)
XAPK       2c7dd2c5b431d95bf84cb033c7e7757d2b53f938cc729fe3b522f3c873000524
Base APK   e1dbde1d57e528bd38b897c5e60c37da016869b47a4a948ee51cdd2baa9cc8c3
Native     a4f8d4d3a3b98b64fca7c32978343a0a003b0997a526f17454120d6fd911687e
Scheme     axonnxtapp
Activity   crc64b0a56c7316c353e7.AuthenticationCallbackActivity (exported)
Notice     assets/dpn/dpn_en.htm (last update 2025-01-16), assets/tou/
Release    assets/release.txt  NXTA-2803
Command    Ottobock_Caa_Commanding_BootLoader_JumpToBootLoaderCommand_get_UpdateType
Command    Ottobock_Caa_Commanding_Slider_WriteSliderPermissionCommand_get_Permission
Auth       Ottobock.Caa.DeviceRemoting.Authentication.SimpleAuthenticator
Telemetry  ObAnalytics_Maui_Targets_NewRelicPlugin_NewRelicHttpClientHandler__ctor
Contacts   apps.austria@ottobock.com, connectgrip@ottobock.com, NAPrivacy@ottobock.com
```

Disclosure Timeline & Outcome

Date	Event
22 Aug 2026	First notice REF OTTOBOCKCONNECTGRIP-2026-R1 sent to apps.austria@ottobock.com, connectgrip@ottobock.com and NAPrivacy@ottobock.com, with the Datenschutzbehörde and the EDPS in copy. The fourth and last part of a family comparison with the notices for Cockpit, connectgo.pro and connectgo. Three questions asked.
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

The permission set is tighter than in connectgo and Cockpit. BLUETOOTH_PRIVILEGED and the legacy storage permissions are not declared, and BLUETOOTH_SCAN carries neverForLocation. There is no boot receiver and no pre-consent content provider beyond the Mono bootstrap and AndroidX startup initialisers. No hardcoded Firebase or Google API key and no secret-shaped token was found. No advertising, session-replay or China-jurisdiction SDK or endpoint is present in the 203 native libraries or the bundled third-party notices, and the only commercial dependency that is not privacy-relevant is Syncfusion's MAUI component suite. Local storage is encrypted with SQLCipher. allowBackup is false, extractNativeLibs is false and targetSdkVersion 34 denies cleartext traffic by default.

The app ships a multilingual privacy notice and terms of use in 14 languages each, with a named controller, a registration number, a named legal representative and both an EU and a US and Canada contact channel, which is more concrete than most apps in this programme provide. The pairing authentication keeps a failure counter, a rudimentary anti-brute-force mechanism at protocol level. The notice states that product data stays on the device.

Residual Risk & Recommendations

Priority	Action	Finding
1	Document where bootloader entry and permission writes are authorised and remove these commands from the patient build or gate them	C1
2	Name the recording and classifier feature, its legal basis and its storage location in the privacy notice	H2
3	Align the Data Safety declaration with the privacy notice and review the label anonymised for device identifiers	H1
4	Confirm PKCE enforcement and align sign-in across the Ottobock apps	H3
5	Name the analytics processor and scope the HTTP instrumentation	M2
6	Add certificate pinning	M1

Residual risk: every copy of version 1.0.53 already distributed contains the command library. This report describes version 1.0.53 only, and the sibling package connectgripna is not covered.

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. 4, 5, 9, 13, 25, 32, 44, MDR (EU) 2017/745 Annex I Section 17.2. RFI-IRFOS ZVR 1015608684, GISA 39261441. REF OTTOBOCKCONNECTGRIP-2026-R1.