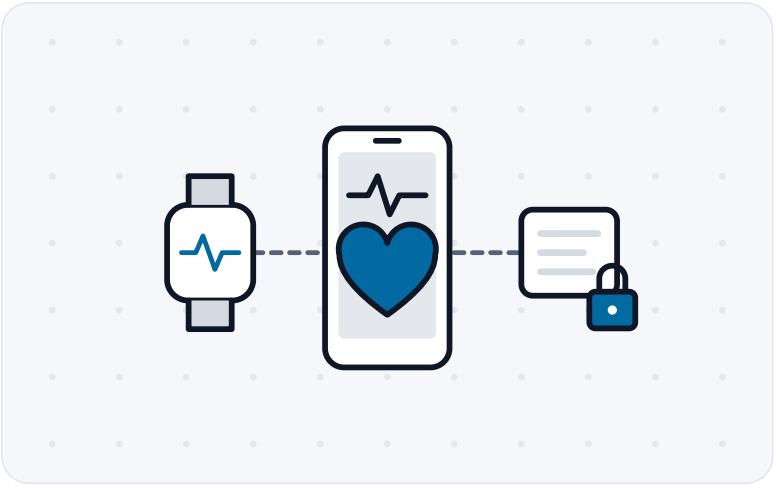
A-SIT Technology
E-Government Innovationszentrum

29. Dezember 2023 Analyse · Mobile Sicherheit · Privatsphäre & Krypto · 12 Min. Lesezeit

Analyse der Android Health Connect Schnittstelle

Gerald Palfinger



Autorinnen und Autoren	Gerald Palfinger
Stand	2023-12-27
Quelle	https://technology2.a-sit.at/veroeffentlichungen/analyse-der-android-health-connect-schnittstelle/

Kernaussagen

- Eine App muss für jede Datenkategorie, die sie über Health Connect liest, die passende Berechtigung deklarieren und aktiv anfordern.
- Beim Erstzugriff fragt Health Connect die Nutzerin bzw. den Nutzer; jede Kategorie lässt sich einzeln für Lesen oder Schreiben freigeben.
- Eine neu installierte App sieht nur die Daten der letzten 30 Tage, damit schädliche Apps nicht auf alle historischen Daten zugreifen.
- Für Health Connect ist eine Datenschutzerklärung Pflicht, und für den Play Store muss der Zugriff bei Google beantragt werden.
- Jeder Zugriff wird protokolliert; die Zugriffe der letzten 24 Stunden sind in den Einstellungen einsehbar.

Auf Smartphones sind in der Regel eine Vielzahl an sensiblen Daten gespeichert. Durch die Kombination mit Wearables und anderen smarten Diagnosegeräten erhalten Smartphones zusätzlich auch noch Fitness- und Gesundheitsdaten, welche detaillierten Aufschluss über den Gesundheitsstatus der Nutzerinnen und Nutzer geben können. Um die Daten besser teilen und analysieren zu können, bieten moderne Smartphone-Betriebssysteme eine zentrale Schnittstelle zur Speicherung sowie zum Abruf dieser Daten an. Durch die Fülle an gespeicherten personenbezogenen Daten sind jedoch der Datenschutz und Sicherheit von höchster Bedeutung. In diesem Bericht wird am Beispiel der unter Android neu verfügbaren Health Connect Schnittstelle gezeigt, welche Schritte für einen Applikationsentwickler notwendig sind, um auf die zentral gespeicherten Fitness- und Gesundheitsdaten zuzugreifen. Ebenso wird aufgezeigt, welchen Einfluss die Nutzerinnen und Nutzer auf den Zugriff auf ihre Daten haben und welche Sicherheitsvorkehrungen vorhanden sind.

1. Einleitung

Durch eine Vielzahl an Sensoren ermöglichen es Smartphones, Fitnessdaten wie die täglich zurückgelegte Schrittzahl aufzuzeichnen. Ebenso werden gesonderte Fitnesstracker und Smartwatches, welche als sogenannte Wearables oft 24 Stunden am Tag am Körper getragen werden, immer beliebter [1]. Diese können eine Vielzahl von Informationen wie Herzfrequenz, Sauerstoffsättigung oder Atemfrequenz aufzeichnen um dadurch relevante Kennzahlen wie Kalorienverbrauch zu berechnen oder beispielsweise Schlafmuster zu erkennen. Ebenso können smarte Haushaltsgeräte wie Personenwaagen weitere relevante Informationen wie Gewicht oder Muskelmasse aufzeichnen. Über Schnittstellen wie Bluetooth Low Energy können diese Geräte mit dem Smartphone verbunden werden. Das Smartphone dient so der zentralen Speicherung der gesammelten Daten. Zum Auslesen der Daten werden jedoch in der Regel herstellerspezifische Applikationen benötigt. Dadurch war es meist so, dass nur die Applikation des Herstellers, welche die Daten vom Gerät abruft, Zugriff auf die jeweiligen Daten hat. Deshalb konnten die Daten von verschiedenen Geräten in der Regel nur gemeinsam analysiert werden, wenn diese Geräte vom selben Hersteller kamen. Um diese Datensilos aufzubrechen, wurden von den Smartphone-Herstellern Schnittstellen entwickelt, welche eine zentrale Speicherung sowie herstellerunabhängigen Zugriff auf die Daten ermöglichen. Eine solche zentralisierte Speicherung kann die Integration verschiedener Gesundheits- und Fitness-Applikationen erleichtern, wodurch bessere Fitness- und Gesundheitsprofile erstellt werden können. Durch die Fülle an gespeicherten Informationen und die zentrale Zugriffmöglichkeit ist die Frage nach Datenschutz und Sicherheit jedoch von höchster Bedeutung. Insbesondere wäre eine detaillierte Zugriffskontrolle, welche den Nutzerinnen und Nutzern die Möglichkeit gibt, einzelne Fitness- und Gesundheitsdaten freizugeben, wünschenswert. In diesem Bericht soll untersucht werden, wie Health Connect unter Android aufgebaut ist, insbesondere im Bezug auf Privatsphäre und Sicherheit der gespeicherten Daten. Dazu wird eine Applikation verwendet, um bereits bestehende Gesundheitsdaten aus einer Applikation auszulesen und in die zentrale Health Connect-Datenbank zu schreiben. Weiters wurde eine separate Applikation entwickelt, welche die Daten wieder aus dem Health Connect-System herausliest. In diesem Bericht wird gezeigt, welche Voraussetzungen eine Applikation zum Lesen der gespeicherten Daten haben muss, wie das System die Zugriffe verwaltet und welchen Einfluss die Nutzerinnen und Nutzer auf die Sicherheit ihrer Fitness- und Gesundheitsdaten haben.

2. Hintergrund

2.1. Health Connect

Sowohl Android als auch iOS bieten einen zentralen Speicherort für Fitness- und Gesundheitsdaten. Während unter iOS mit dem HealthKit SDK dieser bereits mit iOS 8 im Jahr 2014 eingeführt wurde, gibt es einen solchen seit 2022 auch unter Android mit Health Connect. Dabei handelte es sich zuerst um eine eigene Applikation, die über den Play Store installiert werden musste. Mit der Veröffentlichung von Android 14 ist Health Connect jedoch Teil des Systems geworden [2]. Davor konnten Gesundheits- und Fitnessanwendungen ihre Daten nur über applikationsspezifische Schnittstellen wie beispielsweise Content Provider austauschen. Mit Health Connect können nun jedoch Fitness- und Gesundheitsdaten auch unter Android über eine standardisierte Schnittstelle ausgetauscht werden.

2.2. Verwandte Arbeiten

Das Fitnessnetzwerk Strava hat 2018 eine globale Heatmap mit den anonymisierten Streckendaten, welche durch die Nutzerinnen und Nutzer mit ihren Smartphones und Wearables aufgezeichnet wurden, veröffentlicht. Trotz der Anonymisierung der Daten konnten aus der veröffentlichten Heatmap brisante Schlüsse gezogen werden. So konnten über die Daten Stützpunkte von Militärbasen in Krisengebieten erkannt werden [3]. Ebenso konnten einzelne dort stationierte Personen mit Hilfe weiterer Daten aus dem Netzwerk identifiziert werden. Um sensible Standorte zu schützen, hat Strava deshalb eine Funktion zum Verstecken ebendieser eingeführt. Durch diese sogenannten Endpoint Privacy Zonen wird bei hochgeladenen Streckenaufnahmen ein bestimmter Bereich um die sensiblen Standorte versteckt. In [4] wurde jedoch gezeigt, dass diese Methode kaum Schutz bietet. Durch die Verwendung der Eintrittskoordinaten in die Privacy Zone, der angezeigten Distanz der Aktivität, sowie der Straßendaten kann die Wirksamkeit der Privacy Zone erheblich verringert werden. Durch Kombination der Daten kann in einer Vielzahl der Fälle sogar der sensible Standort ermittelt werden. Bei 1,4 Millionen untersuchten Aktivitäten konnte in der Evaluierung etwa 85% der geschützten Standorte deanonymisiert werden.

Darüber hinaus gab es Datenpannen bei verschiedene Online-Fitnessdiensten. So wurden im Jahr 2018 Daten von mehr als 150 Millionen Nutzerinnen und Nutzer des Fitnessnetzwerkes MyFitnessPal geleakt [5]. Im selben Jahr wurde bekannt, dass durch die Fitnessapplikation PumpUp Daten über einen ungeschützten Server zugänglich waren [6]. Darunter fanden sich hochsensible Daten über die Nutzerinnen und Nutzer, neben Namen und Geburtsdaten auch durch die Nutzenden eingetragene Gesundheitsinformationen wie Alkohol- und Tabakkonsum, Medikationen und erlittene Verletzungen. Im Jahr 2020 wurde bekannt, dass durch das Fitnessunternehmen Kinomap mehr als 42 Millionen Datensätze ungeschützt im Internet zugänglich waren [7]. Darunter fanden sich persönliche Details wie Namen, Herkunftsland sowie Informationen über getätigte Trainings. Im Jahr 2021 wurden über 61 Millionen Datensätze von verschiedenen Wearables geleakt [8]. Darunter waren Daten von Fitbit und Apple's HealthKit. Die Daten stammen ursprünglich vom Dienstleister GetHealth, der über seine Applikation Fitness- und Gesundheitsdaten aus verschiedenen Quellen auslesen kann.

In [9] wurde versucht herauszufinden, welche Informationen Nutzerinnen und Nutzer von Fitness-Trackern auf sozialen Netzwerken teilen und wie sich dadurch Dritte ein Bild über ihre Identität machen können. Zur Beantwortung dieser Frage wurde ein Tool entwickelt. Dieses Tool modelliert die Informationen, welche von

den Fitness-Trackern gesammelt und durch die Nutzerinnen und Nutzer in verschiedenen sozialen Netzwerken freigegeben wurden. Dabei zeigt das Tool, welche weiteren persönlichen Informationen in unerwünschter Weise freigegeben werden und welche Datenschutzrisiken dadurch aufgeworfen werden.

In [10] wurde versucht, die Gewohnheiten der Nutzerinnen und Nutzer bei der Weitergabe von Informationen, welche von Fitness-Trackern und anderen Wearables erfasst werden, zu eruieren. Ebenso wurden potenzielle Bedenken erfasst, die sie bei der Weitergabe dieser Informationen über eine Vielzahl von Plattformen haben. Dazu wurden teilstrukturierte Interviews mit insgesamt 30 Teilnehmern durchgeführt. In der Auswertung der Ergebnisse wurde festgestellt, dass Privatsphäre und Sicherheit meist nur eine Nebenrolle bei der Entscheidung spielen, ob potenziell sensitive Fitnessdaten mit anderen geteilt werden sollten. In der Regel basiert die Entscheidung ob gewisse Daten geteilt werden sollen, darauf, welche Ziele die Nutzerinnen und Nutzer im Hinblick auf die Zielgruppen hat, mit der die Daten geteilt werden.

In [11] wurde untersucht, wie die Nutzerinnen und Nutzer die Auswirkungen der Nutzung von Fitness-Trackern auf ihre Sicherheit und Privatsphäre empfinden. Dazu wurde ein Online-Fragebogen ausgearbeitet, um in weiterer Folge in einer Online-Umfrage 212 Nutzerinnen und Nutzer von Fitness-Trackern zu befragen. In der Umfrage wurde festgestellt, dass die Nutzerinnen und Nutzer kaum Schritte einleiten, um die durch ihre Fitness-Tracker erhobenen Daten vor Missbrauch zu schützen. Während sie generell angeben, darüber Bescheid zu wissen, welche Daten durch die Fitness-Tracker erhoben werden, waren sie sich unsicher über die Verwendungsmöglichkeiten der gesammelten Daten. In der Umfrage wurden weiters verschiedene Szenarien abgefragt, die potenzielle missbräuchliche Verwendung im Hinblick auf Privatsphäre und Sicherheit der Daten aufzeigen. Darunter fielen beispielsweise Szenarien wie Identitätsdiebstahl durch Analyse der Fitnessdaten wie zum Beispiel Standortdaten oder die Erkennung einzelner Nutzenden durch die Analyse der Gangart. Während die befragten Nutzerinnen und Nutzer viele der gezeigten Szenarien für möglich hielten, fanden sie, dass es unwahrscheinlich sei, dass diese in der Wirklichkeit stattfinden.

3. Untersuchung

Um die Sicherheitsvorkehrungen der Health Connect-Schnittstelle zu analysieren, wurde eine Applikation erstellt, welche Daten aus Health Connect ausliest. Dazu wurden zuerst Daten einer Personenanalysewaage in die Health Connect-Datenbank geschrieben. Zum Auslesen der Daten aus der Applikation der Waage und zum Hinzufügen der Daten zu Health Connect wurde das Tool „openscale2HealthConnect“ [12] verwendet. Diese Applikation überträgt Daten zu Gewicht, Körperfett und Gesamtkörperwasser zu Health Connect. Im Folgenden wird beschrieben, welche Schritte für eine Applikation notwendig sind, um die dort gespeicherten Daten auszulesen. Da eine potenziell schädliche Applikation in der Regel bereits gespeicherte Daten auslesen will, anstatt neue zu schreiben, liegt der Fokus auf dem lesenden Zugriff. Die Schritte, die benötigt werden, um schreibenden Zugriff zu bekommen sind jedoch ähnlich wie für den lesenden Zugriff.

Damit eine Applikation auf die Fitness- und Gesundheitsdaten zugreifen kann, müssen zuerst die jeweiligen Berechtigungen deklariert werden. Dies geschieht wie bei jeder Berechtigung unter Android im Manifest der Applikation. Hierbei handelt es sich um eine XML-Datei, welche Teil des Applikationspakets ist. In diesem sind neben Informationen über die Applikation auch die durch die Applikation angeforderten Berechtigungen deklariert. Diese werden durch eine eindeutige Bezeichnung identifiziert (beispielsweise

`android.permission.health.READ_BODY_WATER_MASS` zum Zugriff auf Werte der Kategorie Gesamtkörperwasser). Je nach Art der Berechtigung kann es sein, dass das System diese automatisch rein durch die Deklaration im Manifest gewährt. Bei vielen Berechtigungen ist jedoch eine Bestätigung durch die Nutzerin bzw. den Nutzer notwendig, bevor diese von einer Applikation verwendet werden kann. Dies ist auch bei allen Berechtigungen zum lesenden oder schreibenden Zugriff auf Health Connect-Daten notwendig.

Vor dem ersten Zugriff auf Health Connect-Daten muss die Applikation die gewünschten Berechtigungen aktiv anfordern. Dazu erstellt die Applikation ein Set mit den anzufordernden Berechtigungen. Dieses Set wird dem `HealthConnectClient` übergeben. Dabei handelt es sich um die Schnittstelle zwischen der Applikation und dem auf dem Gerät laufenden Health Connect-Dienst. Der `HealthConnectClient` übergibt daraufhin die angeforderten Berechtigungen an den Health Connect-Dienst. Dieser erstellt dann den Berechtigungsdialog, der der Nutzerin bzw. dem Nutzer angezeigt wird. In Abbildung 1 ist ein solcher Berechtigungsdialog ersichtlich. In diesem Dialog haben die Nutzerinnen und Nutzer die Möglichkeit, den Zugriff auf einzelne Datenkategorien zu erlauben oder zu verweigern. Die Berechtigung zum Zugriff kann dabei unabhängig voneinander für den Schreibzugriff und Lesezugriff erteilt werden. In der gezeigten Abbildung versucht die Applikation Lesezugriff auf die Werte Körperfett, Gewicht und Gesamtkörperwasser zu erlangen. Erteilte Berechtigungen können jederzeit durch die Nutzerin bzw. den Nutzer in den Einstellungen des Geräts widerrufen werden.

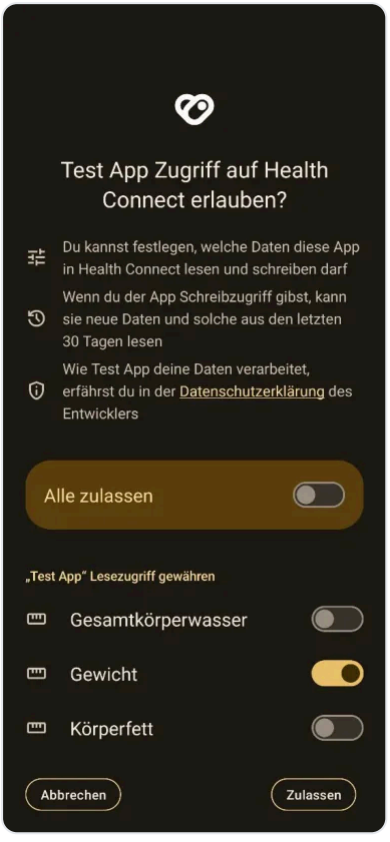


Abbildung 1: Der Berechtigungsdialog von Health Connect ermöglicht es den Nutzerinnen und Nutzern, einzelne Kategorien von Fitness- und Gesundheitsdaten zum Lesen oder Schreiben durch die anfordernde Applikation freizugeben.

Um Health Connect zu verwenden, benötigt eine Applikation zwingend eine Datenschutzerklärung. Diese muss neben den Berechtigungen im Manifest der Applikation deklariert werden. Damit diese der Nutzerin bzw. dem Nutzer angezeigt werden kann, muss die Applikation eine eigene Aktivität deklarieren, welche die Datenschutzerklärung anzeigt. Diese wird über die Aktion `ACTION_SHOW_PERMISSIONS_RATIONALE` ausgeführt, wenn die Nutzerin bzw. der Nutzer die Datenschutzerklärung aus dem Einstellungsdialog von Health Connect öffnet.

Zusätzlich zu den in den vorherigen Abschnitten genannten technischen Voraussetzungen muss zur Veröffentlichung im Play Store der Zugriff auf Health Connect von Google angefordert werden [13]. Dazu muss der Entwickler neben allgemeinen Informationen über die Applikation wie Name und Paketbezeichnung sowie Informationen über sich selbst weitere detaillierte Informationen übermitteln. Dazu zählen neben dem Anwendungsfall der Applikation auch eine Liste der angeforderten Berechtigungen, Begründungen warum diese angefordert werden sowie Kontaktinformationen des Entwicklers. Diese werden ähnlich wie die Applikation selbst durch Google überprüft. Detaillierte Informationen über den Prüfprozess sind jedoch nicht verfügbar.

Erfüllt eine Applikation all diese Voraussetzungen und stimmt die Nutzerin bzw. der Nutzer dem Zugriff auf die Daten zu, so kann die Applikation die Health Connect-Schnittstelle verwenden. Zur besseren Überprüfbarkeit durch die Nutzerin bzw. den Nutzer wird jeder Zugriff einer Applikation auf Daten von Health Connect aufgezeichnet. Die Liste der Zugriffe der letzten 24 Stunden ist in den Einstellungen zu Health Connect ersichtlich. Ein Beispiel dazu ist in Abbildung 2 ersichtlich. Neben der zugreifenden Applikation wird zusätzlich gezeigt, auf welche Kategorie an Fitness- und Gesundheitsdaten zugegriffen wurde.



Abbildung 2: Übersicht über die Zugriffe auf Daten in Health Connect.

4. Fazit

In diesem Bericht wurde gezeigt, welche Schritte Applikationsentwickler gehen müssen, um Daten aus der Health Connect-Schnittstelle unter Android auszulesen. Dabei müssen sie für jede Kategorie an Werten, die ausgelesen wird, die jeweilige Berechtigung anfordern. Beim Erstzugriff auf die Schnittstelle durch die Applikation wird die Nutzerin bzw. der Nutzer nach der Berechtigung für den Zugriff gefragt. Der Nutzerin bzw. die Nutzer hat dabei die Möglichkeit, jede Kategorie individuell freizugeben. Ebenso hat eine neu installierte Applikation nur Zugriff auf die Daten der letzten 30 Tage. Dies sollte verhindern, dass eine potenziell schädliche Applikation Zugriff auf alle historischen Daten erhält. Ebenso müssen Applikationen, die über den Play Store angeboten werden sollten, eine verpflichtende Datenschutzerklärung haben, welche explizit auf die Verarbeitung der abgerufenen Daten aus Health Connect eingeht.

Referenzen

[1] Statista; IDC, „Wearables unit shipments worldwide from 2014 to 2022," 03 2023. [Online]. Available: https://www.statista.com/statistics/437871/wearables-worldwide-shipments/.

[2] Android Developers, „Android 14 - Health Connect," Google Inc, 2023. [Online]. Available: https://developer.android.com/about/versions/14/features#health-connect. [Zugriff am 27 12 2023].

[3] R. Pérez-Peñan und M. Rosenberg, „Strava Fitness App Can Reveal Military Sites, Analysts Say," The New York Times, 2018.

[4] K. Dhondt, V. L. Pochat, A. Voulimeneaso, W. Joosen und S. Volckaert, „A Run a Day Won't Keep the Hacker Away: Inference Attacks on Endpoint Privacy Zones in Fitness Tracking Social Network," in CCS '22: ACM SIGSAC Conference on Computer and Communications Security, Los Angeles, CA, USA, 2022.

[5] D. Lee, „MyFitnessPal breach affects millions of Under Armour users," BBC, 29 03 2018. [Online]. Available: https://www.bbc.com/news/technology-43592470. [Zugriff am 22 12 2023].

[6] Z. Whittaker, „Fitness app PumpUp leaked health data, private messages," ZDNet, 31 05 2018. [Online]. Available: https://www.zdnet.com/article/fitness-app-pumpup-leaked-health-dataprivate-messages/. [Zugriff am 22 12 2023].

[7] P. Muncaster, „Fitness App Kinomap Leaks 42 Million Records/," Infosecurity Magazine, 22 04 2020. [Online]. Available: https://www.infosecurity-magazine.com/news/fitness-app-kinomapleaks-42/. [Zugriff am 22 12 2023].

[8] C. Osborne, „Over 60 million wearable, fitness tracking records exposed via unsecured database," ZDNet, 13 9 2021. [Online]. Available: https://www.zdnet.com/article/over-60-million-recordsexposed-in-wearable-fitness-tracking-data-breach-via-unsecured-database/i. [Zugriff am 22 12 2023].

[9] „Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networksn," in MPS '17: Proceedings of the 2017 on Multimedia Privacy and Security, Dallas, Texas, USA, 2017.

[10] „"There is nothing that I need to keep secret": Sharing Practices and Concerns of Wearable Fitness Data," in USENIX, 2019.

[11] S. Gabriele und S. Chiasson, „Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours," in CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systemsl, 2020.

[12] bahuma20, „ openscale2healthconnect - Synchronize your data from the OpenScale app to Androids Health Connect framework," Github, 2023. [Online]. Available: https://github.com/bahuma20/openscale2healthconnect. [Zugriff am 27 12 2023].

[13] Android Developers, „Request access to Health Connect data types | Android health & fitness | Android Developers," Google Inc, 2023. [Online]. Available: https://developer.android.com/health-and-fitness/guides/health-connect/publish/requestaccess. [Zugriff am 27 12 2023].