

SAMMANSTÄLLD TESTRAPPORT / VERSION 1.1

Formkurvan Live

Klockappens säkerhet

Testrapport och granskning av rättningar

Granskningsdatum och rapportdatum: 13 oktober 2026

Samlad bedömning

De viktigaste bristerna i hanteringen av kontobyte är rättade i den granskade koden. Ett ovanligt fall under en pågående klockaktivitet kvarstår med **låg prioritet**. Granskaren bedömer inte restpunkten som ett hinder för fortsatt utveckling. SÄK-K01 är därför huvudsakligen rättat, men inte tekniskt helt stängt.

Version som bedömningen gäller

Slutligt granskad kod: grenen klocka, commit

2fd38931089402034758109a9907467846c389f0

Grundgranskning: klocka, commit

77d0b8ce82eaccbf1ce9e87d70c9020079b6a2c

Versionssträngen är 0.150 i båda kodversionerna. Commit-id:t, inte enbart versionsnumret, identifierar vad som har granskats.

Område	Slutlig bedömning
Kontobundna uppgifter	Kö, bancache, katalog och rapportörens sparade matchningsutfall rensas. Den aktiva felsökningsflaggan stängs av.
Telefonens motsvarande fel	Körbart omprov visar att gammalt pass avbryts och inte skickar nya rapporter med nästa kontos nyckel.
Klockans pågående pass	Lågprioriterad restpunkt: gammal bana och matchningsunderlag kan överleva kontobytet.
Säkerhetsbedömning	Ingen ytterligare hög eller kritisk brist belagd. Detta är inte ett fullständigt säkerhetsbevis eller ett driftgodkännande.

Rapport-id: G-FKL-K-2026-10-13-R1

Utförd av: G - AI-assisterad granskare (Codex), på Pers uppdrag.

Nytt i version 1.1: rättningen i 8c99a898, K:s rapporterade 242 gröna prov och verifierat riktiga fingeravtryck i 2fd38931. Ersätter version 1.0; ingen ny full testsvit har körts av G.

RAPPORT / 02

Omfattning och arbetssätt

Granskningen gäller säkerhetsgränserna i Formkurvan Lives Connect IQ-klockapp. Uppföljningen omfattar också samma kontobytesmönster i telefonens inspelning. Det är inte en ny granskning av banmatchningens matematiska korrekthet eller alla serverändringar som ingår i slutcommitten.

Granskat område	Kontroll och avgränsning
Parkoppling och nycklar	Personlig enhetsnyckel, återkallande, omparkoppling och hur aktuellt konto bestäms vid sändning.
Lagring och kontobyte	Telemetrikö, bancache, banval, felsökningsflagga och redan inläst tillstånd. Fysisk utläsning ur klockan har inte provats.
Nätverk	Fasta HTTPS-adresser och nyckel i Authorization. Ingen kod hittades som stänger av certifikatkontroll. Ingen avlyssning eller provning av TLS-transporten utfördes.
Baninläsning	Typkontroller och parallella listors längd. Avgränsade felaktiga indata provades; ingen fullständig fuzzning.
Rapportering	Vilka uppgifter som skickas och när tidigare kontos uppgifter riskerar att återanvändas. Serversidans fullständiga åtkomstskydd omfattas av den separata serverrapporten.

Isolerad provning

Exakta kodversioner exporterades till separata lokala kopior. Klockans teststomme använde separat app-id, tillfällig signeringsnyckel och påhittade uppgifter. Serverproven använde syntetiska konton och en tom testdatabas. Telefonens nätanrop ersattes av lokala testsvar. Inga riktiga användaruppgifter eller rapporter skickades till dev eller produktion.

Vad datainsamlingen omfattar

Vanliga rapporter kan innehålla position, puls, höjd, fart, aktivitetstider och matchningsläge. Rapportering kan ske när aktivitetsfältet är öppet, även före Start. Påslagen felsökning kan skicka fler tillgängliga Activity.Info-fält. Detta är inte ett separat konstaterat intrång, men behöver beskrivas korrekt för användaren.

Kön är begränsad i antal, inte i ålder

Taket är 2 000 poster, ungefär 5 timmar och 33 minuter vid en post var tionde sekund. Kön har ingen åldersgräns: kvarvarande poster kan vara äldre. Det är alltså varken obegränsad historik eller ett garanterat femtimmarsfönster.

RAPPORT / 03

Utförda kontroller och resultat

Omgång / version	Vad som kördes	Resultat och innebörd
Grundprov 77d0b8ce	Fyra kompletterande Monkey C-prov i fënix 7-simulatore, SDK 9.2.0.	4 PASS. Två prov bekräftade den dåvarande felaktiga dataöverlevnaden.
Serverunderlag e0556aed	Två kompletterande API-prov och sju befintliga parkopplingsprov.	9 godkända. Bland annat verifierades att gammal rapport accepteras som B när B:s nyckel används.
Telefonrättning fcc31161	Åtta befintliga JS-prov och ett kompletterande kontobytesprov.	9 passerande tester. Det kompletterande provet återskapade ett kvarvarande aktivt pass.
Telefonomprov 01068970	Åtta befintliga JS-prov och omprov av ett återupptaget telefonpass med sen GPS-återkoppling och efterföljande stopp.	9 godkända. Det gamla passet avbryts; inga gamla rapporter skickas med B:s nyckel.
Stödprov 01068970	Ett prov mot projektets JS-kopia av RaceSession.	1 reproduktion. Tomt katalogunderlag släpper inte den redan låsta banan. Inte en Monkey C-körning.
Klockbyggen 51952dfb / 01068970	Fyra respektive sex riktade prov; i senare bygget fyra av K:s och två av G:s. fënix 7, strikt typkontroll (-l 3).	Kompilerade. Inte körda i simulatore av G. Ingen ny kompilering på 2fd38931.
Senaste kontroll 8c99a898 / 2fd38931	Kod- och provgranskning av rapportörens rensning. Alla listade filers SHA-256 jämförda mot Git på slutversionen.	23 av 23 avtryck stämmer. Rensningen bekräftad i kod; inget simulatoromprov av G.

Node-loggen för 01068970 innehåller **10 passerande tester**: nio telefonprov och en reproduktion i JS-kopian. Ett reproduktionsprov passerar när det visar felet. Testantal från olika versioner ska inte summeras till en godkänd fullsvit.

K:s testresultat, inte G:s körning: K rapporterar **242 gröna simulatorprov** samt att proven för inlästa uppgifter och sparat matchningsutfall blir röda när respektive rensning kopplas ur. G har läst provkoden men inte kört dessa prov eller verifierat körloggarna själv.

Begränsning i simulatorunderlaget

Grundprovets logg visar fyra godkända prov, men laddaren gav slutkod 1. Två tidigare försök hade avbrutits före provning; teststommen rättades därefter. Vid omprovningarna togs en befintlig simulator inte över. Resultaten ska inte beskrivas som en felfri fullständig klockgrind.

RAPPORT / 04

SÄK-K01: rättning och restpunkt

Det ursprungliga felet

Efter att A:s nyckel avvisats kunde osända positioner och pulsvärden ligga kvar tills klockan parkopplades till B. Nästa sändning använde B:s nyckel. Servern tilldelade då rapporten till B. Även privata banor och inställningar kunde ligga kvar. Det krävde kontobyte på samma installation, inte ett fjärrangrepp mot ett godtyckligt konto.

Omsändningen efter en ny parkoppling var dokumenterad avsikt i både kodkommentaren och det dåvarande kontraktet. Det som saknades var åtskillnaden mellan samma användare och ett nytt konto. Grundfyndet bedömdes som medelhög risk med begränsad sannolikhet.

Del	Läge vid 2fd38931
Kö och sparad bancache	Rensning tillagd i 51952dfb. Bekräftad genom kodgranskning.
Inläst katalog och diagnostik	Rättat i 211bb179: katalogen töms och aktiv felsökning stängs av. K rapporterar ett kört, falsifierat prov.
Sparat matchningsutfall	Rättat i 8c99a898: lastTickResult och lastTickActivityStart nollställs. Kod och prov granskade; K rapporterar falsifierat prov.
Telefonens kö och aktiva pass	Rättat i fcc31161 och 9497dc6a. G:s omprov på 01068970 visar att passet avbryts utan gamla sändningar.
Klockans redan startade pass	Kvarstår: RaceSession behåller den gamla banan och kan skriva nya matchningsutfall i den tömda rapportören.

Restpunktens praktiska betydelse

Fallet kräver kontobyte medan samma Garmin-aktivitet fortsätter. Nya rapporter använder aktuell position och puls, men gammalt banval och kvarlevande matchning kan följa med. Det är inte återutsändning av A:s rensade positions- och pulskö eller åtkomst till A:s serverhistorik. Restpunkten finns bara på klockan; telefonen avbryter passet och kastar dess rapportör.

Slutlig prioritering: låg. Specialfallet bedöms inte hindra fortsatt utveckling. Den tidigare P2-markeringen ersätts av denna lägre prioritering. K:s överlämning och commit-meddelande dokumenterar Pers beslut att lämna passet tills vidare. Det är ett uppskjutet fynd, inte en tekniskt stängd brist.

Restpunkten bygger på kodspårning, ett tidigare stödprov i JS-kopian och ett kompilerat Monkey C-prov. Ingen full kontobyteskedja på fysisk klocka har provats.

Vanligt täckningsbortfall är ett annat fall

Negativa transportfel återkallar inte nyckeln som HTTP 401 gör. Vanlig offlinekö ska därför behållas. G har granskat och tidigare kompilerat provet för skillnaden, inte själv kört det på slutversionen.

RAPPORT / 05

Spårbarhet och avgränsningar

Exakta kodversioner

Grundgranskning av klockan

77d0b8ce82eaccbf1ce9e87d70c9020079b6a2c

Första klockrättningen

51952dfbc56a2b200098cd5c8958726a8abb97f3

Slutligt granskad klockgren

2fd38931089402034758109a9907467846c389f0

Telefonens första rensning

fcc3116192308149f29e2d83842bcf02e247919d

Telefonens avbrytande av aktivt pass

9497dc6ab643d35631b64f380ff0216a1149bae6

Serverversion i grundprovets API-kontroll

e0556aedfa2f5726834ab50d18ba413373ef63a2

Bevarat granskningsunderlag

[U1] Grundrapport, teststomme, simulatorlogg och serverresultat: [sakerhetsgranskning-klocka-77d0b8ce/](#).

[U2] Första omprovningen: [omprovning-51952dfb/](#).

[U3] Provkällor och Node-logg: [omprovning-01068970/](#).

[U4] Senaste kodkontroll, fingeravtryck och K:s rapporterade resultat: [omprovning-2fd38931/rapport.md](#). U2-U4 ligger under U1.

Kodreferenser: [Kontodata.mc](#), [RaceSession.mc](#), [LiveTelemetryReporter.mc](#) och [telefonklocka.js](#). Länkarna avser slutcommitten och kan kräva behörighet till projektet.

Fingeravtrycksanmärkningen är avslutad

01068970 hade två avvikelser; 8c99a898 hade tre efter ändringen i LiveTelemetryReporter.mc. På exakt 2fd38931 har G jämfört samtliga 23 listade källors SHA-256 med KALLOR.txt: **23 stämmer, 0 avvikelser**. Det avslutar versionsanmärkningen men intygar inte en körd full bygggrind.

Vad rapporten inte intygar

Ingen fysisk klocka, Bluetooth-transport, certifikatvalidering i drift, firmware, fysisk lagringsåtkomst, full FIT-återspelning eller full klockgrind har verifierats i denna granskning. Ingen kontroll av driftsatt version eller juridisk regelefterlevnad ingår. Senare kodändringar omfattas inte automatiskt.

Den tidigare grundrapportens server-SHA hade ett extra tecken. Det korrekta 40-teckens-id:t står ovan. Dokumenten ersätter inte serverns separata säkerhetsrapport. Ingen produktkod har ändrats eller driftsatts av granskaren.

En underlagsförteckning med SHA-256 följer dokumenten. Kontrollsummor visar filidentitet, inte extern certifiering eller digital signering.