SwissCovid Proximity Tracing System - Public Security Test

Aktuelle Meldungen - Notifications actuelles - Notifiche attuali - Current reports

19.10.2020 / 10:00

Security related issues are highlighted in grey.

Number	Date received	Summary / Keyword	Description	Impact	Mitigation	Credits	Status	Remarks
[INR-4173]	28.5.2020	User Experience	Nach Aktivierung der App passiert gar nichts. Nichts verändert sich.	Der Benutzer weiss nicht, ob die App bei ihm überhaupt funktioniert.	Benutzer sollte irgendein Feedback bekommen über die Begegnungen, zumindest die Anzahl am Tag oder einfach ein Zähler, der ständig steigt.		done	Feature request. Selected for development.
[INR-4178]	28.5.2020	Bluetooth setzt Standortfreigabe voraus	Bluetooth ist bei mir standardmässig eh schon aktiv...was ich aber nicht verstehe, ist, warum zusätzlich die Standortfreigabe benötigt wird...die braucht's ja nicht und es kommt schon der Hinweis, dass diese nicht mitgegeben werden...ist es architektonisch bedingt, dass unter Android die Standortfreigabe für die Bluetooth-Kommunikation benötigt wird? Oder warum muss diese aktiv sein?	Muss immer Standort aktivieren...ist bei mir standarmässig immer inaktiv...Bluetooth hingegen ist immer aktiv infolge Smartwatch.	Allenfalls Bluetooth-Kommunikation ohne Standortfreigabe?		done	Duplicate [INR-4610]
[INR-4179]	28.5.2020	API war für ca. 10h blockiert	Anscheinend fragen die iOS-Devices in regelmässigen Abständen bei Apple nach, ob sie sich in Ländern befinden, für welche die COVID-19-API freigeschaltet ist. Mein Testgerät hatte am 27.5 um ca. 10:00 Uhr wohl bei dieser Anfrage den Server von Apple nicht erreicht und folglich die API deaktiviert. Ca. um 20:00 am selben Tag hat das Telefon die API selbständig wieder aktiviert.	Tracing war für ca. 10 Stunden unterbrochen.	Kommunikation mit Apple über deren Verfügbarkeit der Server. Frage nach der Möglichkeit eines man-in-the-middle bei dieser Kommunikation und evtl. den Wunsch nach einer Trägheit für die Deaktivierung des Dienstes beantragen.		done	Issue reported to Apple
[INR-4181]	28.05.20	mise à jour google play	Votre application me demande de mettre à jour Google Play. Ce que j'ai fait. Google Play m'a fourni deux mises à jour, et ne m'en propose plus. Votre application me demande pourtant toujours de mettre à jour google play	Je ne peux pas lancer votre application.			done	Isse not replicable
[INR-4182]	28.05.20	EXPOSURE_NOTIFICATION_API is not available on this device	Installiert SwissCovid Aktiviert Tracing Nach ein paar Minuten erscheint die folgende Fehlermeldung: 17: API: Nearby.EXPOSURE_NOTIFICATION_API is not available on this device. Connection failed with: ConnectionResult{statusCode=UNKNOWN_ERROR_CODE(39501), resolution=null, message=null} Mein Gerät: Android 7.1.2; Fairphone 2 SwissCovid Version 1.0-pilot, 0.5.0	Kein Tracing aktiviert			done	Duplicate of [INR-4195]

[INR-4183]	28.05.20	German Grammar	Was tun, wenn ich ... (Komma, Leerschlag) Bei Symptomen ... (Leerschlag) (generell überall Leerschlag vor ...) Kontaktieren Sie bei Symptomen, die auf das neue Coronavirus hindeuten, Ihren Arzt ... (2 Kommas) Damit können andere Swisscovid-App-Nutzer prüfen, ob sie in den letzten Tagen eine Begegnung mit Ihnen hatten. (Bindestrich; "sie" klein) Erst wenn der Verdacht auf eine mögliche Ansteckung genug gross ist, werden Sie informiert. (Komma; "Sie" gross; "Erst" evtl. streichen)				done	Text modifications applied.
[INR-4185]	28.05.20	Environment variable used for DB password	Based on the docker-compose file (hxxps://github.com/admin-ch/CovidCode-Service/blob/develop/docker/docker-compose.yml#L9) the "db-authcodegeneration" container will use database configuration information based on hardcoded environment variables. Neither should sensitive information like the password be hardcoded in a docker-compose file (please note that this is only relevant in production and the value stored in git is clearly an example password) but in addition environment variables aren't the best fit for this kind of information.	The database credentials could leak to other containers if they e.g. choose link to the "db-authcodegeneration" container. Other data leaking scenarios could be possible but would require more information regarding the underlying infrastructure.	Instead of environment variables, a proper secret management solution should be used (k8s secrets, Docker secrets, Vault, ...).	Disenchant	done	The docker file is provided because that way people can run it locally without DB. The file is not used for anything else. The docker image is documented in the README.md file: https://github.com/admin-ch/CovidCode-Service/blob/develop/README.md
[INR-4186]	28.05.20	Erreur activation fonction de traçage sous Android	J'ai tenté de tester l'application SwissCovid sur un téléphone Honor 10 sous Emui 9. Lorsque je tente d'activer la fonction de traçage je rencontre un message d'erreur : 17: API: Nearby.EXPOSURE_NOTIFICATION_API is not available on this device. (message détaillé en fichier joint)	Impossible d'activer le traçage -> application inutilisation	Rendre l'API disponible sur le téléphone		done	Duplicate of [INR-4195]
[INR-4188]	28.05.20	Debug Logs in Production	The Android mobile app uses "LogLevel.DEBUG" even in production: hxxps://github.com/DP-3T/dp3t-app-android-ch/blob/develop/app/src/main/java/ch/admin/bag/dp3t/MainApplication.java#L49	Debug logs potentially contain too much information that are not needed in production.	The log level should be reduced to e.g. info.	Disenchant	done	These logs are only used during the pilot phase. They will be deactivated for the public release.
[INR-4190]	28.05.20	Weak Content Security Policy	The CovidCode-UI Content Security Policy (CSP) uses the 'unsafe-inline' directive (even for production): hxxps://github.com/admin-ch/CovidCode-UI/blob/master/src/nginx/csp_headers-prod.conf#L1	A proper Content Security Policy can make the exploitation of e.g. Cross-Site Scripting (XSS) attacks way harder. The used 'unsafe-inline' directive drastically reduces this additional layer of defense.	Remove the 'unsafe-inline' directive from the CSP.	Disenchant	done	With Angular it is not possible to avoid unsafe-inline with the style-src directive. But this is only for the CSS, meaning no script can be executed.
[INR-4191]	28.05.20	Text abgeschnitten	Der Titel in einem der Screens ist nicht vollständig dargestellt (Siehe Anhang)				done	Issue reported to Google
[INR-4193]	28.05.20	Geht nicht mehr	Obwohl ich alles freigebe geht die App nicht mehr	Kein Schutz kein tracing			done	Issue not replicable
[INR-4194]	28.05.20	Process in Docker container running as root	The "dp3t-sdk-backend" ws Docker image is adding a new user "ws" (hxxps://github.com/DP-3T/dp3t-sdk-backend/blob/develop/ws-sdk/Dockerfile#L11) but all further actions including the final launch	In case of a successful attack a least privileges approach can potentially prevent further harm to the overall system.	A low privilege user should be used instead of root.	Disenchant	done	For details of implemented fix see: https://github.com/DP-3T/dp3t-sdk-backend/pull/127

			of the Java application is performed by the root user. In addition the ADD directive in hxxps://github.com/DP-3T/dp3t-sdk-backend/blob/develop/ws-sdk/Dockerfile#L25 should ideally be replaced by a COPY directive but it's not too relevant as long as only a trusted local file is added to the Docker image.					
[INR-4195]	28.05.20	Tracing - 17: API: Nearby EXPOSURE_NOTIFICATION_API	Aktivieren des Tracing endet mit dieser Meldung. Bluetooth deaktivieren - Tracing aktivieren - Meldung betreffend Bluetooth - Bluetooth aktivieren - Tracing ist aktiv für ca 30 Minuten, danach stürzt das ab. Die geforderten Berechtigungen sind alle zugelassen. Gerät Nokia 7.3 Android ONE, Modell TA-1196, Android Version 10, Details siehe Anhang	Tracing ist deaktiviert			done	Solution has been implemented by Google and been distributed within Switzerland.
[INR-4196]	28.05.20	Keine Kontaktmeldungen mehr	Meldung erhalten.	anscheinend funktioniert es nicht mehr			done	Issue not replicable
[INR-4197]	28.05.20	Bessere Information, welches Betriebssystem benötigt wird	Erst beim Installieren des Testflight wird man darauf hingewiesen, dass man das wirklich allerneueste Betriebssystem (iPhone , ios 13.5) braucht, um die App zu laden. Das müsste man vorher schon bekannt geben. Ich wollte die App kurz vor dem Nutzen des ÖV laden und musste das verschieben, weil ich erst lange warten musste, bis mein iPhone die >900MB ios 13.5 runtergeladen hatte.	So vergeht einem die Lust auf die neue App.	angeben, dass die allerneueste Version des Betriebssystems benötigt wird!		done	This is not connected to the app but to the iOS updates process in general.
[INR-4198]	28.05.20	Feature request Bluetooth/Airplane mode	Android: Wenn das Handy in den Flugmodus gesetzt wird, so alarmiert die App, dass Bluetooth nicht eingeschaltet ist. Das kann man zwar nachvollziehen, da ich aber in der Nacht immer auf Flugmodus umstelle, bzw. im Flugzeug auch BT abgeschaltet werden muss, macht die Alarmierung keinen Sinn.	Störende Alarmierung, dass BT nicht eingeschaltet ist (in der Nacht, im Flugzeug, im Kino etc.). Unter Android bietet die Notification settings der App ausschliesslich das komplette Abschalten an.	Granularere Einstellmöglichkeiten, was Alarmiert werden soll und was nicht. Und/oder im Flugmodus generell keine Alarmierung		done	Feature request reported to Google
[INR-4199]	28.05.20	Proximity Tracing unmöglich	Die App wurde auf das Huawei-Telefon heruntergeladen und auch durch das Startmenu durgeführt erst bei dem Einschalten der Tracing Funktion ist es zu einem Error gekommen.		Huawei-Telefon auch akzeptieren		done	Issue not replicable. Not enough information.
[INR-4205]	29.05.20	IOS - Benachrichtigungen Deaktiviert	Die App hat super funktioniert, bis vorgestern. Seither sieht es aus als App? Meine Region abgeschalten hat. Komisch.				done	Issue not replicable. Not enough information.
[INR-4208]	29.05.20	Activity Indicator	With the App closed it is not visible if the tracking is active or not. A small sign in the head bar of the smartphone or lockscreen could inform the user about the actual state of the App.	User could forget to reactivate the App.			done	Feature request, implementation to be decided

[INR-4218]	29.05.20	Läuft die app?	Es ist mir nicht ersichtlich ob die app läuft. Muss die app im "recent apps" offen sein oder läuft sie immer auch wenn ich die app da rauskicke. Die app zeigt keine meldung wenn ich Bluetooth abschalte.	Unklarheit ob app macht was sie soll	Symbol in der statusleiste oder notification über appzustand (läuft: symbol wird angezeigt, läuft aber kein Bluetooth: symbol angezeigt aber durchgrstrichen, läuft nicht, kein symbol). Meldung der app falls bluetooth abgeschaltet wird (sind sie sich sicher, da dadurch die app nicht mehr funkt)		done	Duplicate to [INR-4208]
[INR-4219]	29.05.20	Covid-Tracing not able to activate due to error	Error when trying to activate tracing. And tracing stops without action.	not able to start tracing.			done	Issue not replicable. Not enough information.
[INR-4220]	29.05.20	API Error	Nach der Installation der App hat die App dem Anschein nach fehlerfrei funktioniert. Nach einem De- und Reaktivieren der Tracing Funktion ist einige Minuten später (Gerät wurde dazwischen gesperrt) die Tracing Funktion von automatisch deaktiviert worden. Beim Versuch das Tracing manuell wieder zu aktivieren ist eine API Error aufgetreten (siehe Screenshot). Informationen zum Testgerät: -Modell: Honor 10 COL-L29 -Build Nummer: 9.1.0.357	Tracing ist nicht möglich. Hauptzweck der App nicht verfügbar.		captain	done	Duplicate to [INR-4195]
[INR-4225]	29.05.20	Fehlermeldung API	Tracking lässt sich nicht aktivieren. Fehlermeldung: 17: API: Nearby.EXPOSURE_NOTIFICATION_API is not available on this device. Connection failed with: ConnectionResults(statusCode=UNKOWN_ERROR_CODE(39501), resolution=null, message=Null). Habe Google Play Service upgedatet ohne Erfolg, danach Google Play Service gelöscht, neu installiert, ohne Erfolg.	Tracking lässt sich nicht aktivieren.			done	Duplicate to [INR-4195]
[INR-4237]	29.05.20	Tracing kann nicht aktiviert werden	App konnte heruntergeladen und installiert werden. Das Tracing kann jedoch nicht aktiviert werden. Fehlermeldung: 17: API: Nearby.EXPOSURE_NOTIFICATION_API is not available on this device. Connection failed with: ConnectionResult{statusCode=UNKNOWN_ERROR_CODE(39501), resolution=null, message=null} Gerät: HUAWAI P30 lite, Android-Version 10 SwissCovid: Version 1.0.1-piolot, 0.5.1	Tracing wird nicht aktiviert			done	Duplicate to [INR-4195]
[INR-4239]	29.05.20	Malicious applications can communicate with the broadcast receiver	Call to registerReceiver [:52] misses the broadcastPermission argument - no permissions will be checked for the broadcaster, which allows a malicious application to communicate with the broadcast receiver.			DeepCode.ai	done	This broadcast receiver is only used as a trigger to check for the latest state of the SDK. It does not interprete any data. Therefore no fix needed.

[INR-4240]	29.05.20	Current use of java.util.Random yields no properly randomly distributed numbers.	To guarantee any random distribution, there should be one class Random generator class and "nextInt" should be called on it. By creating one generator every time, there is no guarantee that the numbers will be properly randomly distributed.	Since the currently implemented process will not provide fully random numbers this could be exploited by an attacker who knows that this is the case (Open Source Code)	Just create one Random object and reuse it.	DeepCode.ai	done	Fixed. Code was modified accordingly and deployed.
[INR-4238]	29.05.20	Missing close on java.io.FileInput Stream leads to a resource leak.	In /DP-3T/dp3t-sdk-backend on line 82 you have as Missing close on java.io.FileInputStream [:82] leads to a resource leak. Which could lead to more serious problems as well.		Just close the resource.	DeepCode.ai	done	Fixed, for details of implemented fix see:https://github.com/DP-3T/dp3t-sdk-backend/pull/128
[INR-4241]	30.05.20	Nicht alle Komponenten sind Open Source	Die aktuelle Version der APP funktioniert nicht ohne GAEN und das ist nicht Open Source. In Art 8.4 der Verordnung zu der APP steht aber: "Der Quellcode und die technischen Spezifikationen aller Komponenten des SPTS sind öffentlich".	Auf e.foundation und vielen anderen Open Source Handys nicht nutzbar, wie man in hxxps://github.com/DP-3T/dp3t-app-android-ch/issues/60 sehen kann.	Auch eine Version ohne GAEN API unterstützen. Die Versionen ohne GAEN funktionieren, aber solange diese nicht offiziell unterstützt werden und so mit den GAEN Versionen synchronisiert sind, sind sie praktisch wertlos.	Timon Zielonka	done	Directly answered to reporter. Will be added to the FAQ.
[INR-4246]	30.05.20	Probleme mit Bluetooth Speaker Iphone	Seit Installation der App auf dem Iphone wird die Musikwiedergabe mit Spotify über einen externen Bluetooth Speaker immer wieder unterbrochen. Deshalb werde ich die App mal wieder deinstallieren und ich hoffe, ihr könnt das Problem mit Apple zusammen lösen.				done	Issue not replicable. Not enough information.
[INR-4252]	30.05.20	Server nicht erreichbar ASST 404	Trotz bestehender Internetverbindung (Sie erhalten ja auch dieses Feedback) ein Fehler erhalten.	Kein Abgleich möglich			done	This is related to a known downtime.
[INR-4253]	30.05.20	Verbindung mit Internet funktioniert nicht mehr	Meldung ASST404, Internet-Verbindung funktioniert nicht mehr, obwohl eingeschaltet				done	Duplicate [INR-4701]
[INR-4255]	30.05.20	Benachrichtigun g	Seit 4 Tagen habe ich die App installiert. Heute bekomme ich die Mitteilungen, das keine Internetverbindung besteht. Mein Handy ist aber sowohl zu Hause mit WLAN wir auch unterwegs mit 4G verbunden. In der App kann ich diesbezüglich ja auch gar nichts einstellen.	Mitteilungen mit Standard Benachrichtigungs-Ton. Keine Möglichkeit, dieser Meldung irgendwie Folge zu leisten.			done	This is related to a known downtime.
[INR-4279]	01.06.20	Falsche Fehlermeldung bei ungenügendem Smartphone Speicherplatz	Wenn der Smartphone Speicherplatz zur Neige geht erscheint wiederholt die Fehlermeldung "keine Internetverbindung"	wiederholte Fehlermeldungen, weitere Auswirkungen nicht feststellbar.	Löschen von unbenötigten Daten wie Fotos etc.		done	Selected for development
[INR-4280]	01.06.20	Benutzerfreundli chkeit	Ich vermisse den Comic mit der Erklärung der Funktionsweise, welcher vor ein paar Wochen im Umlauf war. Ich meinte, der kam von der ETH Zürich. Und war sehr anschaulich. Mich stört gewaltig, dass GPS eingeschaltet werden muss, macht in Innenräumen auch kaum Sinn				done	Feature request, implementation to be decided

			und wenn ich das Tracing stoppe, zum Bsp. über Nacht alleine zu Hause, würde ich es schätzen, wenn die App eine Option hätte, gleichzeitig auch Bluetooth (und GPS) abzuschalten. Gerne würde ich auch prüfen oder zumindest mittels einer Übersicht sehen können, was mein Gerät bereits gesammelt hat. Falls ich keine Möglichkeit habe, zumindest etwas über die Sammeltätigkeit der App zu erfahren, werde ich sie nur sehr ungern benutzen.					
[INR-4281]	01.06.20	SwissCovid unterstützt unsichere Bluetooth Protokolle	SwissCovid App unterstützt alte Bluetooth Protokoll Versionen (4.0 und 4.1). BTLE gilt aber erst mit Version 4.2 als sicher. Zum Beispiel werden auf den älteren BTLE Versionen die Schlüssel ungeschützt übertragen und man kann "mithören." Benutzer der SwissCovid App mit alten Mobilgeräten (2014 und älter) werden nun "gezwungen" sich mit einer potentiell unsicheren offenen Schnittstelle in die Öffentlichkeit zu begeben. Es kann natürlich auch auf Bluetooth Stacks Version 4.2 Vulnerabilitäten geben. Das ist schwieriger zu erkennen und den Schaden dort zu begrenzen.	Die SwissCovid App selber hat kein Problem damit. Man nötigt den Benutzer aber eine unsichere Schnittstelle am Mobile zu öffnen. Wenn ich sehe wer ältere Mobilgeräte betreibt, sind das meistens Personen die sich der Gefahr nicht bewusst sind.	Die App könnte lediglich Bluetooth ab Version 4.2 unterstützen oder ein Hinweis bei der Installation anzeigen, dass eine unsicheres Betriebssystem verwendet wird.		done	This is a general issue of the Bluetooth protocol and not specifically of the SwissCovid App. This issue can therefore not be fixed.
[INR-4282]	31.05.20	Keine Ahnung ob App läuft	Sehe nicht ob App korrekt läuft. Kein Feedback. Keine Ahnung...	Scheint, dass App nicht geht. Dann deinstallieren wir sie halt wieder?	Z.B. Ein Zähler der zB pro Tag getroffene Personen mit convid App oder Anzahl Stunden pro 24h wo App aktiv war, etc wäre nötig => gab es Unterbrüche?	Stellina	done	Duplicate of [INR-4280]
[INR-4306]	02.06.20	téléchargement de l'application	j'ai voulu télécharger votre application afin de la tester et je n'ai pas pu le faire car je n'ai pas la dernière version d'iOS.	je n'ai pas pu télécharger l'application	De nos jours, les iPhones sont vite obsolètes et supportent mal les mises à jour. Il serait bien de faire une application accessible à tous, même avec d'anciennes versions du système d'exploitation.		done	Duplicate of [INR-4197]
[INR-4323]	02.06.20	bug	Les problèmes sont les suivants:: 1. Le traçage ne peut pas s'activer sous Android EMUI 9.1.0 (la mise à jour me dit: Votre logiciel est à jour). Tél. Honor "Play" avec correctif sécurité avril 2020. 2. "Le bouton à glissière" pour activer le traçage ne fonctionne pas de façon logique: Quand on clique dessus, il bascule d'état et affiche un message d'erreur dans une fenêtre, indiquant que le traçage ne peut pas être activé. Quand on pousse la glissière vers la droite pour l'activer, le bouton devient bleu (comme si l'action est validée), mais le traçage est toujours désactivé, SANS le message d'erreur dans la fenêtre. 3. sur cette page de rapport, le rébus après les informations personnelles n'est pas clair: il indique chez moi: 5 * 7 * ce qui ne veut ien dire. Voulez-vous dire "5 * 7 =" pour attendre la	Le comportement décrit ci-dessus sous 1. et 2. rend l'application inefficace. Pour être utile, l'App doit s'installer sans problème sur le plus grand nombre de smartphones sans accrocs. A défaut, son utilisation restera anecdotique et inutile pour un traçage des contacts.	Corriger l'activation du traçage pour fonctionner sur tous les smartphones de moins de 3 ou 4 ans. Le mien n'a qu'environ 2 ans. Merci de me tenir informé quand les problèmes sont résolus.		done	Selected for development

			réponse 35 ??? J'ai indiqué 35, eet cela est refusé... 4. Le bouton "Send en n'est pas traduit en français.					
[INR-4324]	02.06.20	L'application crashe	Sur mon téléphone (Sony XPeria Z2, Android 6.0), l'application crashe systématiquement avec l'erreur "EXPOSURE_NOTIFICATION_API not available" (cf capture ci-jointe), sans doute parce que c'est un vieil OS. Après avoir reçu une demande de mettre à jour Google Play (???) et l'avoir fait, j'ai retesté, y compris sur la dernière version disponible. Même résultat sur la même erreur. Vu que l'erreur réapparaît continûment, j'ai désinstallé l'application	L'application est inutilisable	Assurer que SwissCovid ne s'installe que sur les versions supportées, ou au moins lister celles-ci...	Goldor0ck	done	Duplicate of [INR-4195]
[INR-4344]	03.06.20	Hyfenation in english	Hyphenation used in the instruction at the beginning after downloading the app in the first screens (in English language).	Minimizing the use of hyphenation in Instruction for Use is a recommendation for medical devices' instruction for use. Though it's not totally a medical device. The readability is slightly impacted by hyphenation.	Remove all the instances of hyphenation in the app text.		done	Feature request, implementation to be decided
[INR-4345]	03.06.20	Service wird unbemerkt beendet beim Schliessen der App	Wird die App manuell beendet, z.B. via "alle Apps schliessen", wird auch der Service beendet. Daran zu erkennen, dass keine Notification erscheint, wenn Bluetooth deaktiviert wird. Honor 9 (Huawei STF-L09), Build 9.1.0.210	Der Benutzer merkt nicht, dass das Tracking nicht mehr aktiv ist. Er wird nicht benachrichtigt, dass das Tracking nicht mehr möglich ist.	Der Service muss weiterlaufen, auch wenn die App beendet wird. Das Tracking soll dann, und nur dann, wenn der Benutzer dieses manuell deaktiviert auch beendet werden. Vergleichbar mit dem Service einer Messenger-App (wobei dies nicht bei allen gleich gut funktioniert), der ja auch Nachrichten empfängt wenn die App geschlossen wird.		done	Issue reported to Google
[INR-4346]	03.06.20	Lack of UI feedback	The App lacks visual feedback if it's set correctly and ready to function. Nothing tells you that the app is ready and has all the authorization (notification, background app refresh etc.)	Red is the color of Switzerland but it's the color of errors as well or "stop". The banner at the top is red, could be interpreted as an error signal or as if your app is still not working.	Change the color of the banner to green or blue when the app is all set and ready to be used with all the authorization of the phone (bluetooth on, notifications set, background refresh enable etc.)		done	Duplicate of [INR-4280]
[INR-4365]	04.06.20	Swiss Covid App in Grenznähe	Ich lese nirgends Verhaltensregeln für Bewohner in Grenzgegenden (Basel, Genf, Tessin etc.). In diesen Regionen verkehren täglich tausende von Grenzgängern. Wie sollen sich Bewohner dieser Gegenden verhalten? Können die verschiedenen Länder-App (Deutschland, Frankreich, Österreich, Italien) miteinander kommunizieren? Oder sollen Bewohner dieser Gegenden sicherheitshalber die App der Nachbarländer auch installieren? Behindern sich diese App nicht gegenseitig?	Auswirkung, wenn verschiedene Länder-App auf dem Smartphone installiert und aktiv sind. Allenfalls rechtliche Konsequenzen?	Es sollte möglicherweise getestet werden, wie sich verschiedene Länder-App miteinander verhalten, wenn sie gleichzeitig installiert sind. Information an Bewohner der Grenzregionen.		done	Directly answered to reporter. Will be added to the FAQ.

[INR-4389]	04.06.20	Sprache	Es gibt, oder sie ist nicht leicht zu finden, keine Möglichkeit die Appsprache abweichend von der Systemsprache des Telefons zu Konfigurieren.	Einige Begriffe werden nicht verstanden.	Möglichkeit zur Sprachwahl implementieren		done	Feature request, implementation to be decided
[INR-4391]	04.06.20	Unzureichende Kontraste	Die Kontrastverhältnisse zwischen Text und Hintergrund sind auch bei erhöhtem Kontrast auf dem iPhone nicht ausreichend.	Gemäss WCAG 2.0/2.1 muss das Kontrastverhältnis zwischen Text und Hintergrund mindestens 4.5:1 bestehen, damit Menschen mit Sehbehinderung die Inhalte gut wahrnehmen können. Es darf zudem nicht davon ausgegangen werden, dass alle User auch wissen, wo sie den erhöhten Kontrast aktivieren können.	Kontrast erhöhen	allerlay	done	Feature request, implementation to be decided
[INR-4392]	04.06.20	Überschriften sind nicht als Headings ausgezeichnet	Auf der Infoseite alle Überschriften korrekt ausgezeichnet. Auf den übrigen Seiten fehlt diese Auszeichnung. Sehende erkennen die Überschriften an der fetten und farbigen Schrift. Für VoiceOver-Anwender präsentiert sich alles einfach als Textabschnitt.	Blinde und sehbehinderte iPhone-Anwender bedienen das Smartphone mithilfe des integrierten Screenreaders «VoiceOver». Du kannst VoiceOver ebenfalls in den Einstellungen aktivieren. Mithilfe von speziellen Gesten kannst du dann auf dem Touchscreen navigieren. Eine beliebte Funktion ist das Anzeigen von Überschriften. Ähnlich wie beim Navigieren auf einer Website, können iPhone-User auf diese Weise den Inhalt «querlesen» und von Überschrift zu Überschrift springen, ohne sich alles vorlesen zu lassen.	Überschriften korrekt als H1, H2 etc. auszeichnen.	allerlay	done	Feature request, implementation to be decided
[INR-4393]	04.06.20	Inkonsistente Auszeichnung der externen Links	Dies geschieht beim FAQ-Button vorbildlich: Der Linktext informiert den User darüber, dass man bei Klick die SwissCovid-App verlässt und sich ein Fenster im Browser öffnet. Bei allen anderen Links fehlt diese Information, obwohl ein Icon für Sehende darauf hinweist.	Linktexte sollIten gemäss WCAG 2.1 die Anwenderinnen und Anwender jederzeit über das Linkziel und Funktionen informieren.	Externe Links korrekt auszeichnen und nicht nur visuell mit dem Icon.	allerlay	done	Feature request, implementation to be decided
[INR-4394]	04.06.20	Uhrzeit	Wenn man wie einige Personen, die Handyzeit 5 min zu früh hat, meldet die App immer einen Fehler. Ich würde einen Zeitrahmen von +-10 min einbauen, die App weiss so oder so, ob man 15min bei jemandem gestanden hat oder nicht, da spielt die genaue Uhrzeit auch kein Problem.	App funktioniert nicht	Uhrzeit mit +-10 min Toleranz.		done	Feature request, implementation to be decided
[INR-4434]	05.06.20	Incompatibility with requirements, inconsistent information, critical privacy issues	Submission of a report (Analysis of SwissCovid) with the following main topics: - SwissCovid is not open source and under the control of Apple-Google. - Some information are not correct. There are misconception about anonymity, encryption, and open source. - Bluetooth allows easy surveillance. - Reporting diagnosed users can be identified. - False at-risk notifications can be injected. - Self-injection is possible.	- Sovereignty under threat. - Mistrust by users. - Surveillance by third parties. - Privacy issues for reporting users. - People may be sent to quarantine maliciously. - People can abuse subsidies.	- More transparency is required: - switch to true open source - make information sincere - rethink the Bluetooth approach - consider other protocols such as DH-based - consider protections against replay attacks - make sure covidcode and JWT cannot be sold	Serge Vaudenay	done	15.06.20: Risk assessment for replay attacks published 17.06.20: Security Issue Submission [INR-4434]. Detailed analysis published
[INR-4462]	07.06.20	Verfügbarkeit der App	Die App sollte unbedingt (auch) auf einer Schweizer Webseite (des Bundes) zum Download zur Verfügung gestellt werden! Schliesslich geht es keine ausländische Firma wie Google etwas an, wer diese App auf sein Gerät lädt (man braucht dafür ja einen persönlichen Account!)!	Wirklich Datenschutz-bewusste Personen verzichten auf das Downloaden der App von den "allgemeinen" App-Stores... = geringere Verbreitung der App	App auf der BAG-Seite (ebenfalls) zum Download anbieten! Herzlichen Dank!		done	It is not planned to distribute the app outside the Google- and iOS App-Store.

[INR-4471]	07.06.20	iOS: Region für Kontaktmitteilun gen geändert	Direkt nach der Installation der App habe diese Meldung bekommen: "Region für Kontaktmitteilungen geändert. COVID-19 - Kontaktmitteilungen werden von "SwissCovid" in dieser Region möglicherweise nicht unterstützt. Du solltest in "Einstellungen" bestätigen, welche App du verwendest." Modell: iPhone 11, iOS: 13.5.1, App 1.0.2	Die Meldung erscheint immer wieder. Ich habe bereits alle Einstellungen geprüft, kann aber keinen Fehler finden.			done	Issue reported to Apple
[INR-4549]	09.06.20	Standort-Funktion aktiviert?!	Ich bin zwar nicht Teil der Testgruppe, habe mir die App aber schon einmal installiert. Dabei habe ich gesehen, dass neben Bluetooth auch die Standort-Funktion aktiviert sein muss. Das wurde bisher nicht so kommuniziert und erläutert und ist für mich weder nachvollziehbar noch akzeptabel.	Die Standort-Funktion ist bei mir normalerweise deaktiviert und das wird auch so bleiben. Für alle mündigen und kritischen Smarphone- resp. Mobile-Nutzerinnen und -Nutzer bedeutet dies wie für mich ein Showstopper. So werde ich die App nicht nutzen. Für mich ist die Akzeptanz der App äusserst fraglich.	Standort-Funktion bleibt von der SwissCovid-App unangetastet, d.h. die App funktioniert auch mit deaktiviertem Standort-Funktion.		done	Duplicate [INR-4178] This issue cannot be fixed because Android does not separate Bluetooth and GPS activation. Will be reviewed again
[INR-4554]	09.06.20	Disinformation attacks	Possible Replay attacks.. 1. It is possible to seed in real life the phones of hundreds of people with beacons coming from hundreds of others. If one of the individuals whose beacons was "inserted" is later marked as infected, reflecting his/her genuine status, that would then trigger a lot of notifications, that would all be false positives. 2. I believe it is possible to get some retroactive location information for people who have been marked as at risk, using a side database. For instance it should be possible to infer where those people live, or where they work. 3. I believe the entire system, including its deployment, its backers, etc is subject to disinformation attacks. The very nature of this protocol makes its utility to grow very slowly with the installation rate. However the "attack surface" for the two types of attacks above grow much faster. Update 18.06.20: Full report submitted.	Disinformation attacks		Paul-Olivier Dehaye	done	15.06.20: Risk assessment for replay attacks published The NCSC considers the risk in this case as acceptable.
[INR-4556]	09.06.20	swisscovid iphone 6plus	L'applic nécéssite ios 13.5.1 pas installable sur cet iphone. C'est le cas de 80% des iphones.				done	Duplicate [INR-4197]
[INR-4610]	10.06.20	GPS Deaktivierung stoppt die App	Wie schon mit INR-4178 gemeldet, benötigt die App auf einem Android-Gerät (entgegen den ursprünglichen Angaben/Deklarationen!) neben einem permanent aktivem Bluetooth AUCH ein permanent aktive Standortfreigabe (GPS). Die Formulierung (Zitat) "This issue cannot be fixed because Android does not separate Bluetooth and GPS activation" ist falsch, bzw. irreführend, da: - auch auf einem Android-Gerät Bluetooth und Standord-Freigabe auf Ebene des UIs beim Endanwenders sehr wohl unabhängig de-/aktiviert werden können. - auch die gezielte Deaktivierung der reinen Standord-Freigabe nach Installation + Start der	Auch wenn die App die Freigabe angeblich nicht benötigt, muss die Standort-Freigabe weiterhin permanent aktiv sein -> für viele Sicherheitsaffine Endbenutzer und allem was bzgl Google bzgl. Standort bekannt ist ein NoGo.	(optimal): auch für Android-Benutzer reine Bluetooth-Nutzung ohne Standort-Freigabe. Da scheint es doch Möglichkeiten zu geben: siehe bspw. https://stackoverrun.com/de/q/9105172 (minimal) Transparenz in der Deklaration was die App auf welcher Plattform tatsächlich benötigt!		done	

			App sofort dazu führt, dass die App wieder nicht mehr aktiv ist.					
[INR-4621]	10.06.20	Verbindungen die nichts mit Covid zu tun haben	Meine Firewall zeigt Verbindungen der App zu Seiten wie abcnews.go.com oder charts.finanzen100.de an. Die restlichen Verbindungen zu pt.bfs.admin.ch oder codegen-service.b inag.admin.ch sehen legitim aus.	Vertrauen der Bevölkerung in die Legitimität der App ist beschränkt, wenn die sich zu irgendwelchen Webseiten verbindet. Wie soll da noch Anonymität gewährleistet sein?	Keine Verbindungen zu nicht *.admin.ch Webseiten.		done	False positive. Incorrect assignment of packets by the Android firewall
[INR-4646]	11.06.20	Tracing deaktiviert trotz Bluetooth und Ortung	Trotz aktiviertem Bluetooth und Ortungsdienst kommt es in der App wiederholt zu der Meldung "Tracing deaktiviert" (siehe screenshot-Anhang "SwissCovid_screenshot_meldung.png") und beim Versuch zu "Aktivieren" zum Fehler wie im screenshot-Anhang "SwissCovid_screenshot_fehler.png" ersichtlich. Die "leserliche" Fehlermeldung ist unvollständig.	Da es keinen systematischen workaround zu dem Problem gibt und die App in dem Zustand unbrauchbar ist, werde ich sie wieder deinstallieren.			done	Google has fixed this bug
[INR-4653]	11.06.20	Fehlermeldung	Beim Öffnen der App erschien ein unerwarteter Fehler mit Angabe eines Fehlercodes. (IJWTSE4). Ursache nicht eruierbar. App ansonsten normal bedienbar.	Keine Auswirkungen festgestellt. Fehlermeldung verschwand einige Minuten später wieder.			done	Caching problem. Was fixed in backend deployment (1.0.3)
[INR-4657]	11.06.20	Synchronisation error notifications	I get the following error for a couple of hours already: "L'application ne peut pas fonctionner correctement: Une erreur inattendue s'est produite lors de la synchronisation des notifications. (AGAEN39508)" Android 7.1.2, Fairphone 2 SwissCovid Version 1.0.2-pilot, 0.5.2				done	This problem has been fixed.
[INR-4658]	12.06.20	compliance mit idee des gesetzestextes	Eine open source app die auf einem reinen opensource android smartphone nicht läuft, weil zwingend der google play store benötigt wird, ist irgendwie nicht wirklich open. AWS als CDN ist auf fragwürdig. Eine verteilung der software nur über die US amerikanischen stores von google und apple ist auch fraglich, wieso kann das BIT keine direkten downloads ermöglichen? und wieso ausgerechnet bluetooth? Sicherheitslücken, ungenaue distanzmessungen, und und und...	schreckt ab. nicht sehr vertrauensfördernd. oder sogar komplett unbrauchbar.			done	See publications on: https://www.melani.admin.ch/melani/de/home/public-security-test/current_findings.html • Risk-Estimation-Proximity-Tracing_Appendix_Signed • NR-4434_NCSC_Risk_assessment
[INR-4668]	12.06.20	Fehlermeldung	Mir wurde folgende Mitteilung angezeigt: Region für die Kontaktmitteilungen geändert. Danach habe ich die App geöffnet und sie zeig unter Meldungen: ein unerwarteter Fehler ist aufgetreten.	Es ist nicht klar, ob die App weiterhin funktioniert. Keine Anweisungen ob User-Interaktion nötig ist			done	Duplicate [INR-4718]

[INR-4670]	12.06.20	Keine aktuellen Daten	Fehlermeldung: Es ist ein unerwarteter Fehler beim Synchronisieren der Meldungen aufgetreten (AGAEN39508)				done	Duplicate [INR-4657]
[INR-4686]	12.06.20	Bluetooth ohne GPS	Android-App: 1.0.2-pilot, 0.5.2, Android 7.0: Wenn ich das GPS ausschalten, bekomme ich ständig eine Meldung bezüglich Bluetooth. Wenn der Standort der App sowieso nicht mitgeteilt wird, sollte Bluetooth auch unabhängig von GPS funktionieren. Bitte nachbessern.	Man könnte sich fragen, ob Google hier nicht zu stark schnüffeln könnte. Denken viele Leute so, würde das der Akzeptanz der App im der Bevölkerung schaden.			done	Duplicate [INR-4178]
[INR-4688]	12.06.20	Fehlermeldung	Die App gibt via Benachrichtigung den Fehler AGAEN39508 aus. Mangels weiteren Informationen scheint die Funktionalität nicht gegeben.	Tracing funktioniert nicht?	Nett wäre eine Feedback-Möglichkeit direkt aus der App heraus.		done	Duplicate [INR-4657]
[INR-4689]	12.06.20	App verlangt GPS	Die App meldet, dass sie zur Zeit nicht richtig funktioniert, da die Standortinformation ausgeschaltet ist und deshalb Bluetooth nicht verwendet werden kann.	Ich werde die App deaktivieren. Ich will keine Software auf meinem Smartphone die Einstellungen verlangt, welche angeblich nicht verwendet werden. Solche Praktiken werden von unseriösen Anbietern benutzt.			done	Duplicate [INR-4178]
[INR-4690]	12.06.20	Erreur d'horloge	Depuis ce samedi 12, environ 18h, erreur répétée plusieurs fois par heure. Arrêt forcé, redémarrage, sans succès.				done	Duplicate [INR-4657]
[INR-4701]	13.06.20	Cannot connect to the server	Today at approx 6PM I received a push notification saying that "App currently unable to function properly [...] Please check that your device is connected to the internet (ASST502)" My internet connection works fine. I cannot tell whether this is a security vulnerability (that is, if an attacker can cause this issue), but the app is apparently not functioning properly.	If the message is correct, the app is not synchronizing. I have no way to verify whether this is true. As such, I marked the severity as Medium.			done	Due to planned backend maintenance.
[INR-4704]	13.06.20	Keine Internetverbindung	Die App meldete mehrmals, dass die Uhrzeit des Telefons nicht richtig ist und sie eingestellt werden muss. Dies ist jetzt nicht mehr der Fall, aber es erscheint die Meldung, dass die Daten seit langem nicht mehr synchronisiert werden konnten. Das Problem besteht gemäss Meldung daher, dass das Telefon keine Internetverbindung haben soll. Dies hat es aber die ganze Zeit.				done	Duplicate [INR-4657]
[INR-4705]	13.06.20	Erreur lors de la synchronisation	Le message suivant s'affiche : L'application ne peut pas fonctionner correctement : une erreur inconnue s'est produite lors de la synchronisation des notifications (AGAEN39508)				done	Duplicate [INR-4657]
[INR-4708]	14.06.20	Absturz	App ist abgstürzt				done	Not enough information
[INR-4716]	14.06.20	Warnhinweis bei der Installation der App	Hat man die App aus dem AppStore runtergeladen und öffnet sie, erscheint ein Warnhinweis. Die Verwendung sei nur für berechtigte Personen für den Testlauf gestattet. Warum dies, wenn doch im Fernsehen bereits	Viele Leute wagen sich ab hier nicht mehr weiter.	Soll die App zukünftig von vielen Leuten eingesetzt werden, muss besser abgestimmt werden zwischen Kommunikation und Hinweisen in der App.		done	During the test phase there is a limited group of users.

			der Spot läuft, die Öffentlichkeit könne die App verwenden?					
[INR-4717]	14.06.20	Für iPhone 6 nicht verwendbar.	Da beim iPhone 6 nur bis iOS 12 ein Update besteht, kann die App nicht runtergeladen werden. Sie erfordert eine höhere Version.	Schränkt die Anzahl Benutzer drastisch ein. Nicht jeder verfügt über die neuesten iPhones.			done	This is not connected to the app but to the iOS updates process in general.
[INR-4718]	14.06.20	Fehlermeldung	Beim Öffnen der App Fehlermeldung, die später wieder verschwindet. (ENErrorDomainfehler-13)				done	Due to maintenance.
[INR-4726]	14.06.20	Verbindungsproblem	Die App meldet Internetprobleme, obwohl alle anderen Apps funktionieren. Ich vermute, Wartungsfenster werden nicht korrekt erkannt.				done	Duplicate [INR-4657]
[INR-4782]	16.06.20	Unbekannte Fehlermeldung bei Kontaktmeldungen	Seit einigen Tagen erscheint diese unerwartete Fehlermeldung in meiner App unter der Rubrik, wo allfällige kritische Kontakte angezeigt werden sollten (siehe Secreenshot). Die Fehlermeldung läst sich nicht öffnen oder entfernen.	Ich weiss nicht, ob ich benachrichtigt werden würde, falls ich mit einer infizierten Person in Kontakt war.			done	Duplicate [INR-4718]
[INR-4802]	16.06.20	Batterienutzung iPhone	Die Swiss COVID App selber braucht wenig Batteriekapazität (1%). Das durch iHealth abgeglichene Kontaktprotokoll deutlich mehr (12-18%) in den letzten Tagen.	Batterielaufzeit iPhone	Rückmeldung an Apple?		done	Issue not replicable. Not enough information.
[INR-4893]	18.06.20	Nutzung in Grenznähe	Als Arbeitgeber in der Grenzregion zu Deutschland und auch mit hohem Exportanteil und damit internationaler Kundschaft ist es wichtig, dass die Swiss Covid App das Tracing auch mit anderen Länder Apps (z.B. deutsche Corona-Warn App) sicherstellt.				done	This issue is being discussed.
[INR-4952]	21.06.20	Generation of false negatives	Assume an attacker uses a phone to capture a beacon in a room, modify it into several others and rebroadcast all those derivatives in the same room. Through the SDK/botnet attack, the attacker actually doesn't need to be physically present in that room (or Switzerland). The modification of the beacon is done via the AEM tampering attack of Vaudenay and Vuagnoux. Multiple beacons are actually generated, and by targeting specific bits the attacker can make sure to generate equally spaced metadata values by powers of 2. So 2^n beacons spaced 2^(8-n) apart, including the original one. The Apple doc says https://developer.apple.com/documentation/exposurenotification/enexposureconfiguration: """ The attenuation (transmission power - RSSI) can vary during an exposure event. Attenuation values >0 are weighted by the duration at each risk level and averaged for the overall duration.	This multiplication of beacons would lead to a different weighted average, which depending on the details could falsely move the risk level into the safe territory.	This seems to be a weakness of the Google/Apple API. It is hard to devise a mitigation given that we don't have clarity on how the average is computed.	Paul-Olivier Dehaye	done	The risk has been analyzed. The NCSC considers the risk in this case as acceptable. The risk assessment must also take into account whether there is a benefit and ROI for someone who takes advantage of it.

			The framework measures and calculates this value. """ The risk levels seem to be: A > 73 db, 73 >= A > 63, 63 >= A > 51, 51 >= A > 33, 33 >= A > 27, 27 >= A > 15, 15 >= A > 10, A <= 10 so intervals of size 54,10,12,18,6,12,6,10 (note how strange the intervals are, but they are the same for Google) Note that the Apple doc is ambiguous when you actually want to compute what that gives in practice. 23.06.20: Additional remark Three papers that might be additionally relevant to the assessment, because they talk about the averaging in more details (and also the opacity of it): https://www.scss.tcd.ie/Doug.Leith/pubs/gaen_verification.pdf https://down.dsg.cs.tcd.ie/tact/pairwise.pdf https://down.dsg.cs.tcd.ie/tact/replay.pdf Some of it focuses on replay attacks (for false positives), but this might also be helpful to better understand the potential for false negatives.					
[INR-5021]	22.06.20	Fehlermeldung	Ich habe mehrmals in der Testphase die Mitteilung bekommen, dass die "Region für Kontaktmitteilungen geändert" worden sei und Kontaktmitteilungen in der Region möglicherweise nicht unterstützt würden. in den Einstellungen solle ich bestätigen, welche App ich verwende. In den Einstellungen war dazu aber nichts zu bestätigen/auszuwählen.	Diese Nachricht habe ich alle paar Tage erhalten. Auswirkungen: Es war mir überhaupt nicht klar, wie ich damit umgehen soll. In den Einstellungen war dazu nichts zu bestätigen/auszuwählen. Unklar blieb, ob das Tracing nun nicht funktioniert.	Falls etwas zu tun ist: Mitteilung so ändern, dass klar ist, WAS zu tun ist und ob das die Funktionalität beeinträchtigt (und wenn ja wie).		done	Duplicate [INR-4471]
INR-5198	26.06.20	Rolling Proximity Identifiers are traceable	The Rolling Proximity Identifier (RPI) is not synced with the random BD_ADDR when updated. Thus, the user can be traced as if the RPI was fixed. Description: An adversary is sniffing (passively) Bluetooth broadcast messages from smartphone using GAEN (for example Swisscovid). Because BD address and RPI are not modified at the same time, the user of the app can be traced indefinitely (instead of at max 15 minutes). We called this attack 'Le Petit Poucet' (Der Kleine Däumling) because the user lets some 'small stones' (e.g. de-synchronized broadcasts) to identify the new Rolling Proximity Identifiers (RPI) and the new random BD address.	An adversary passively listening Bluetooth broadcast is able to trace continuously the user of the Swisscovid app (and it shouldn't).	Update the value of the BD address and the RPI at the same time to avoid the critical 'small stone' Bluetooth packet. This is probably related to GAEN.	Martin Vuagnoux	analysis	The risk has been analyzed.. Synchronizing the Bluetooth address with RPI only works if the underlying Bluetooth stack (chip/firmware etc.) supports it. This is not the case with older devices. The NCSC considers the risk in this case as acceptable
INR-5205	26.06.20	EphID's update interval fixed, tracing possible	As the EphID's update interval time is fixed, tracing is therefore possible because if one	Uses can be tracked/traced as long as continuous, interruption free monitoring is possible (e.g. in a store)	change EphID on a random time interval	romeokienzler	done	The risk has been analyzed. The NCSC considers the risk in this case as acceptable. The risk assessment must also take into

			EphID appears and another disappears so you can guess that they belong together Please see our discussion at https://github.com/DP-3T/documents/issues/69					account whether there is a benefit and ROI for someone who takes advantage of it.
INR-5251	28.06.20	Fake Key Service	Several problems with fake key service may lead to the possibility to distinguish fake from real keys.	This makes the use of fake keys pointless			done	The issue has been analyzed and discussed. The NCSC considers the risk in this case as acceptable.
INR-5573	08.07.20	Bluetooth Sicherheit und Corvid-App des Bundes	Seit einiger Zeit ist ja bekannt, dass es bei (einigen Typen) Android-Geräten eine Sicherheitslücke bezüglich Bluetooth gibt.. Diese Sicherheitslücke besteht offenbar bei Handys, die noch nicht mit dem Betriebssystem Android 10 (Q) ausgestattet sind; also bei Handys die unter Android 8 oder 9 laufen. Diese Sicherheitslücke besteht ganz allgemein beim Bluetooth; also auch, wenn z.B. via Bluetooth-Kopfhörer Musik gehört wird. Solange Bluetooth aktiviert ist, könn(t)en dann, wenn ich richtig informiert bin, Kriminelle, die sich in der Nähe befinden, via Sicherheitslücke Codes auf dem Android-Smartphone ausführen, ohne dass der rechtmässige Nutzer des Smartphones dies mitbekommt und so z.B. Schadprogramme, "Spionageprogramme" etc. installieren.. Da die Corvid-App des Bundes Bluetooth zur Ortsbestimmung nutzt und die User der Corvid-App Bluetooth permanent eingeschaltet haben - und dies ja auch einer breiten Öffentlichkeit bekannt ist - könnten kriminelle Hacker diese Sicherheitslücke "im grossen Stil" ausnutzen..	Ich möchte einfach zu bedenken geben, was passieren könnte, wenn Kriminelle via - wegen der Corvid-App - permanent eingeschalteter Bluetooth-Verbindungen beispielsweise in Firmenhandys eindringen könnten oder Passwörter stehlen bzw. abfangen würden etc.....			done	Duplicate [INR-4281]
INR-6786	13.08.20	Zugang zu ausgetauschten Daten mit user COVID19 app	Durch die app COVID-19 kriegt man sehr schnell und einfach die Daten von andren user durch dem Bluetooth Austausch kriegt man date wie: user ID Anzahl ausgetauschten Daten + zeit warnend Daten Austausch, Anzahl angesteckten Personen.	Es ist erschreckend das man so schnell und einfach Zugang zu solchen Daten bekommt. Mit bessere hinweissen könnte man noch tiefer in die Daten reinschauen.	Datenschutz rechte verbessern.		done	
INR-7913	16.09.20	Update on 4674 Malevolent SDK	I have previously submitted a report to NCSC/Melani concerning SwissCovid. It was tagged as case 4674. Today I provide an update, in the form of a peer-reviewed paper accepted for publication at a well-known conference on privacy and security.	I have previously submitted a report to NCSC/Melani concerning SwissCovid. It was tagged as case 4674. Today I provide an update, in the form of a peer-reviewed paper accepted for publication at a well-known conference on privacy and security. Together with my co-author, we show, among other things: 1. we show and detail one SDK and associated apps that could monitor and interfere with GAEN/SwissCovid 2. the extreme ease through which existing SDKs could be converted to conduct attacks against GAEN/SwissCovid, and acquire necessary permissions on Android 3. we detail a new type of passive attack, which we call a biosurveillance attack	There is no good mitigation, except monitoring of mildly popular apps for the acquisition of new Bluetooth-related permissions. For popular apps already having those permissions, one could demand legally-backed guarantees on how such data is exploited	Paul-Olivier Dehaye	done	Follow Up of [INR-4952] The risk has been analyzed. The NCSC considers the risk in this case as acceptable. However, we are continuously monitoring the current developments of the threat situation, including the observation described here.

INR-8418	05.10.20 Updated at 08.10.20	Replay Attacks of Reported Keys	We successfully implemented a replay attack on SwissCovid of reported keys, which triggers a false notification on the victim smartphone. Date and time of smartphone can be modified using a rogue NTP server, a fake base station or a fake GNSS signal. The chosen date corresponds to a real infection, retrieved from a daily TEK list. In the proximity of the victim, the attacker sends continuously an RPI generated from the available TEK list (and the corresponding date and time). After 10-12 minutes, the smartphone has saved the RPI into its database (this can be verified with adb logcat). UPDATE 08.10.20: The attacker can speed up the attack by controlling the time of the smartphone (3 scans of 5 seconds are sufficient). We successfully performed the attack in less than 30 seconds instead of 10-12 minutes. When the date and time is set back to normal on the smartphone, SwissCovid shows a possible infection notification.	We can trigger false alert in the proximity of the attack (around 50-100m because the Bluetooth power threshold is faked) UPDATE: 08.10.20: The attacker needs to share the Wi-Fi network or set a fake base station to modify the date and time.	When date and time is changed, double check before accepting RPIs.	Vincenzo Iovino, Serge Vaudenay and Martin Vuagnoux	done	We are continuously monitoring the current developments of the threat situation. The NCSC considers the risk in this case as acceptable. The risk assessment must also take into account whether there is a benefit and a ROI for someone who takes advantage of it. Especially since an attacker typically must be on site.