# IT-beveiligingsbedrijf Secura vindt inconsistenties in broncode CoronaMelder


**Op verzoek van het ministerie van VWS doen IT-bedrijven onderzoek naar de veiligheid van de app voor corona-contact=opsporing, de CoronaMelder. Dat zijn: NFIR, Secura, Radically Open Security, Privacy Management Partners en FoxIT. Sinds vandaag, 29 augustus 2020 staat het rapport van het IT-beveiligingsbedrijf Secura.B.V. op de website van de Tweede Kamer. Daarin staat dat de app wel voldoet aan een aantal vereisten, zoals verwoord op pagina 4 en 5 van het rapport, maar toch inconsistenties bevat. Deze zijn weliswaar klein(minor), maar zijn uit het oogpunt van cybersecurity toch niet bepaald onbelangrijk.** Ook waarschuwt Secura voor een potentieel probleem bij een onderdeel dat niet onder haar opdracht viel, maar waar een ander bedrijf over gaat. Dat gaat over de zogenaamde backend-voorziening. Vanuit de eigen expertise waarschuwt men dat daar een potentiële kwetsbaarheid aanwezig is door het tegelijkertijd aanwezig zijn van de tijdelijk blootstellingscodes en het IP-adres van de gebruiker.

## Samenvatting

Aangezien het om een aantal zeer technische zaken gaat die zich moeilijk in kort bestek laten vertalen druk ik hierbij de hoofdpunten uit de managementsamenvatting af. Het rapport heeft overigens als publicatiedatum 19 augustus 2020.

*As a result of the source code review Secura has ascertained that the iOS and Android versions of the applic atiOil adhere to security and privacy requirements. However, Secura found a*

*number of minor inconsistencies while assessing the application's source code.*

## Inconsistentie 1

Secura constateert verouderde software bij de iPhone-versie van de CoronaMelder:

1. *The iOS application makes use of a software library that implements transport security and other cryptographic functions, in a version (vi.1.1D) that is not the most recent version and Is known to contain vulnerabilities. The vulnerable parts of the library are not used by the app however,. therefore there is no impact to security or privacy. However using the most recent version of libraries that do not contain any known vulnerabilities is always recommended, especially when future versions of the app might contain code that does call vulnerable parts of the library.*

## Inconsistentie 2

Men vervolgt met commentaar op het niet goed controleren van digitale handtekeningen:

2. *Some cryptographic signatures used to validate the keys that unlock exposure notifications (so-called Temporary Exposure Keys, or TEK's), are only partially checked. As a result all holders of a certificate recently issued by KPN as part of the PKI-Overheid service, could in theory produce valid signatures. This partially violates the integrity requirements defined in the architecture. However. because TEKs are protected in transit by a TLS connection and are also protected by an additional cryptographic GAEN-signature Secura was not able to identify a scenario where this flaw could be practically exploited by an attacker.*

## Inconsistentie 3

Secura gaat verder met commentaar op het niet herkennen van door gebruikers gemodificeerde besturingssystemen van smartphones.

3. *The app does not perform a check to see if it is running on a rooted or jailbroken device. Running any app on a rooted (Android) or jailbroken (iOS) device introduces security and privacy risks and can harm the integrity of all apps and communication. Not all users with a rooted or jail broken device might be aware of this. A warning to users trying to install the app on a rooted or jailbroken device could make them aware of the additional risks.*

## Inconsistentie 4

Tenslotte meldt Secura nog een item over “lokaas-berichten”:

4. *Decoy messages are sent in order to make it more difficult for attackers to gather any meaningful information from any messages. However, when the app is disabled. decoy messages are still sent. This is not fully in compliance with the functional requirements and under specific circumstances could help an attacker identify users of the app even if it is disabled.*

## Ronald Prins

De voormalige CEO van het IT-beveiligingsbedrijf Fox-IT liet op Twitter vandaag meteen weten toch wel even te schrikken dat de digitale handtekeningen niet goed gecontroleerd worden. Dat gaat om inconsistentie 2 hierboven. Dankzij andere maatregelen is dat niet te misbruiken, maar het zou toch niet mogen.

## Root en jailbreak

Er bestaat een groep smartphone-gebruikers die graag het eigen besturingssysteem ervan kraakt, Bij Android-toestellen gaat het om het zogenaamde “rooten”. Bij iPhone-gebruikers gaat het om de “jailbreak” van het IOS-besturingssysteem. Deze mensen lopen met hun smartphone veiligheids- en privacy-risico’s. Zij krijgen(zie inconsistentie 3) geen waarschuwing. Technisch is het mogelijk dat de app kan constateren dat het om een gemuteerd toestel gaat en de gebruiker waarschuwen. Dat doet de CoronaMelder niet.

## Niet vlekkeloos

Het rapport van Secura maakt duidelijk dat er aan meerdere dingen toch niet goed gedacht is ondanks de aandacht die het ministerie zegt te hebben voor een vlekkeloze app. Men moet zich wel bedenken dat het onderzoek dat nu voorligt maar een deel van de systematiek betreft. Andere IT-beveiligingsbedrijven moeten over andere onderdelen nog hun oordeel naar buiten brengen, o.a. over het door mij hierboven genoemde backend-probleem van de CoronaMelder(zie pagina 7 van het rapport.) Daarbij kan potentieel een tijdelijke besmettingscode aan een individueel persoon gelinkt worden.

Het één en ander laat wel zien dat het “eventjes” een nieuwe vlekkeloze app bouwen die voor alle Nederlanders zou moeten gaan werken er niet bij is.

W.J. Jongejan, 29 augustus 2020

Afbeelding van iXimus via Pixabay