Auteur: Comité Interfédéral Testing & Tracing
Sujet: Rapport en réponse à une possible atteinte de la vie privée par Google GAEN
Date: 27 avril 2021

Que s'est-il passé?

Google et Apple ont développé ensemble une technologie décentralisée d'alerte d'exposition dans le cadre de la lutte contre le COVID-19. Cette technologie porte le nom complet de Google Apple Exposure Notification, ou GAEN en abrégé. L'application belge Coronalert utilise GAEN, tout comme des dizaines d'autres applications dans d'autres pays, avec plus de 100 millions de téléchargements au total.

L'implémentation du GAEN par Google fait que trop d'informations sont stockées dans de logs ou journaux du smartphone. Plus précisément, deux catégories d'informations sont stockées :

1. Les clés de l'utilisateur même (aussi nommé rolling proximity identifiers, RPIs)
2. Les clés partagées (ou RPIs) et les adresses MAC Bluetooth temporaires des contacts

Quelles sont les implications ?

Certaines applications, dites "privilégiées", sont autorisées à lire les données stockées dans les logs ou journaux sur les appareils Android. Il s'agit principalement d'applications qui ont été préinstallées sur le téléphone par les fabricants de matériel, les opérateurs de réseau et leurs partenaires commerciaux. Cela peut se faire, entre autres, dans le cadre des rapports de crash.

Sur base de ces informations, des parties tierces pourraient déterminer le statut d'une personne (positive ou non), ou le risque auquel elle a été exposée. Dans le cas extrême, les données pourraient être croisées, ce qui permettrait de reconstruire les interactions entre personnes et pourrait permettre d'identifier des individus ou de les localiser.

Pour les utilisateurs d'iPhone qui entrent en contact avec des utilisateurs d'Android, il existe également un risque (plus faible).

Ce problème, qui relève de la responsabilité de Google, a été signalé par à Google par des chercheurs le 19 février 2021. Il a été rendu public le 27 avril 2021.

Il n'y a pas d'indication que des applications "privilégiées" auraient recueilli ces informations sensibles ; pour autant que Google puisse en juger, elles ne l'ont pas fait.

Les compagnies dont il s'avèrerait qui ont utilisés ces données de logs risquent une amende.

Comment est-ce que ceci est remédié?

- Google a indiqué que le déploiement de la mise à jour d'Android est en cours.
- Le déploiement de la mise à jour Android se terminera dans les prochains jours.
- Le DPO de Sciensano a informé l'autorité de protection des données.

Comment l'IFC Testing & Tracing protège-t-il la sécurité et la confidentialité de Coronalert?

- L'Autorité des Protections des Données a été consultée avant le lancement de Coronalert
- L'utilisation de Coronalert repose sur une base légale
- Coronalert utilise une technologie DP3T,respectueuse de la vie privée, où les décisions sont prises de manière décentralisée et où le moins d'informations possible sont partagées avec des tiers
- Le code source de l'application est disponible publiquement (transparence)
- Des audits de sécurité ont eu lieu lors de la création ainsi que lors de modifications techniques majeures