KPMG

Security onderzoek Corona apps

Test scenario's / aspecten
19 April 2020

Scenario's die we getest hebben door gelimiteerde initële penetratietest

1. Een kwaadwillende is in staat om gevoelige data te verkrijgen uit de opslagruimte van applicatie X op het mobiele apparaat van de eindgebruiker. Dit scenario kan zich voordoen als het mobiele apparaat kwetsbaar is en applicatie X gevoelige data (bewust of onbewust) op slaat op het apparaat. Hierdoor kan de privacy van de gebruiker alsmede mogelijke andere gebruikers (als hierover ook data is opgeslagen doordat deze gebruikers in de buurt waren) worden aangetast.
2. Een kwaadwillende is in staat om de communicatie tussen applicatie X en de achterliggende infrastructuur te onderscheppen en/of te misbruiken (het kanaal zelf of bijvoorbeeld via de API). Dit scenario heeft een hogere kans bij het gebruik van publieke hotspots zoals guest Wi-Fi en/of publieke hotspots.
3. Een kwaadwillende is in staat om communicatie tussen applicatie X en de achterliggende infrastructuur te compromitteren door misbruik van andere kanalen dan het primaire kanaal (de te verwachten API-interface). Denk hierbij aan aanvullende kanalen zoals e-mail, SMS of andere TCP/UDP interfaces.
4. Een kwaadwillende is in staat om de achterliggende infrastructuur van applicatie X te compromitteren of ernstig te verstoren door het injecteren van kwaadaardige code. Hierdoor kan de beschikbaarheid, integriteit en vertrouwelijkheid van het systeem en data niet worden gewaarborgd.
5. Een kwaadwillende kan gevoelige informatie bemachtigen door het ongeautoriseerd kunnen communiceren met de achterliggende infrastructuur van applicatie X.
6. Een kwaadwillende is in staat om foutieve data in te brengen of correcte data te verwijderen door misbruik van de achterliggende infrastructuur van applicatie X. Hierdoor wordt de data in de achterliggende infrastructuur minder betrouwbaar en kan niet meer goed worden bepaald welke gebruikers COVID19 infectie hebben en welke niet.

Aspecten die we onderzocht hebben door middel quickscan broncode onderzoek

1. Wat is het algemene beeld van broncode van de applicatie met bekende metrieken als LOC
2. Worden er door automatische tooling reële kwetsbaarheden van de Betrouwbaarheid en Beveiligbaarheid in de broncode gevonden?
3. Zijn er andere data-uitgangen (back-doors) (inclusief logging) dan gedefinieerd in de broncode te vinden?
4. Is de geleverde software (zowel front-end als back-end) voor de goede werking afhankelijk van externe bibliotheken? Zo ja zijn deze bibliotheken courant, worden ze onderhouden en/of bevatten ze bekende kwetsbaarheden van de Betrouwbaarheid en Beveiligbaarheid?
5. Is de broncode opgezet in lijn met onze verwachtingen vanuit de technische en functionele documentatie? (Zijn bijvoorbeeld beschreven privacy mechanismen geïmplementeerd, past de omvang bij de beschrijving, etc.)