NKSC prie KAM
Inovacijų ir mokymo skyrius
support@ims.nksc.lt

2020 – 10 – 27

Mobiliosios aplikacijos „KoronaStopLT“ kibernetinio saugumo vertinimas

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC) atliko kompleksinį Nacionalinio visuomenės sveikatos centro (toliau – NVSC) užsakytos mobiliosios aplikacijos „KoronaStopLT“ (toliau – Aplikacija) kibernetinio saugumo vertinimą. Aplikacija skirta sekti koronavirusinės infekcijos „COVID-19“ kontaktus panaudojant skaitmeninę kontaktų sekimo technologiją. Ši aplikacija realizuota „iOS“ ir „Android“ platformose.

Tyrimo metu atlikta detali Aplikacijos kodo „iOS“ ir „Android OS“ platformų atvejais ir serverio programinių sprendimų analizė, įvertintas skaitmeninės kontaktų sekimo technologijos saugumas, atlikti Aplikacijos kuriamų duomenų srautų stebėjimai, belaidžio ryšio trakto matavimai. Tai leido nustatyti potencialias Aplikacijos ir jos infrastruktūros kibernetinio saugumo grėsmes, pateikti produkto saugumą didinančias korekcines įžvalgas ir rekomendacijas tolesnei jo plėtrai.

PAGRINDINĖS TYRIMO IŠVADOS

Tyrime buvo nagrinėti NVSC pateikti programiniai paketai: „Korona Stop LT“ aplikacija, skirta „Android OS“ operacinės sistemos įrenginiams (aplikacijos versijos Nr.: 0.1.3, sisteminis identifikatorius: „lt.nvsc.coronawarnapp“), „iOS“ įrenginiams skirta „KoronaStopLT“ aplikacija (aplikacijos versijos Nr.: 0.0.4, sisteminis identifikatorius: „lt.nvsc.coronawarnapp“) ir „KoronaStopLT“ serverio programinė realizacija „cwa-server“ (versijos Nr. 1.3).

Nustatyta, kad „Korona Stop LT“ aplikacija, skirta „Android OS“ įrenginiams, nereikalavo prieigos teisių prie įrenginio duomenų ar funkcionalumo. „iOS“ skirta „KoronaStopLT“ aplikacija reikalavo trijų leidimų: leidimo gavus pranešimą jį atvaizduoti (ir apie tai vartotojui pranešti garsiniu signalu), leidimo aplikacijai dirbant foniniame rėžime siųsti ir gauti duomenis tinklo traktu ir juos apdoroti, leidimo aplikacijai naudoti „Pranešimų apie galimą kontaktą su COVID-19 užsikrėtusiu“ (orig. *ExposureNotification*) asmeniu karkasą. Galima teigti, kad nagrinėtų „KoronaStopLT“ aplikacijų reikalavimai įrenginio prieigai yra racionalūs ir būtini jos funkcionavimui.

Funkcionavimui „KoronaStopLT“ aplikacijos naudoja viešai prieinamą „Decentralizuotą privatumą išsaugantį atstumo sekimo“[1] protokolą „DP-3T“ (angl. *Decentralized Privacy-Preserving Proximity Tracing*), parengtą 2020 m. balandžio mėn. tarptautinių mokslininkų iš dvylikos institucijų. Protokolas pasižymi tuo, kad informacija, reikalinga skaitmeniniam kontaktų sekimui, yra saugoma vartotojo įrenginyje, ir privatūs duomenys trečiosioms šalims nėra prieinami. Šio protokolo praktinė realizacija – „Google“ (Alphabet Inc.) ir „Apple“ (Apple Inc.) korporacijų sukurtas programinis produktas „Exposure Notifications“, kurio pagrindu veikia „KoronaStopLT“ aplikacija.

Atlikus detalią „KoronaStopLT“ naudojamo protokolo „DP-3T“ analizę nustatyta, kad jis sukurtas principu, leidžiančiu išvengti asmeninių ar privačių duomenų rinkimo ir saugojimo procedūrų, o jo

[1] Projekto specifikacija ir technologinė dokumentacija. https://github.com/DP-3T/documents

praktinėje „Exposure Notifications“ realizacijoje šio principo yra tvirtai laikomasi. Nepaisant korektiško protokolo funkcionavimo vartotojų duomenų saugumo kontekste, nustatyti šie potencialiai taisytini kibernetinio saugumo neapibrėžtumai:

1. Galimas sergančiųjų skaičiaus klastojimas. Sergančiųjų vartotojų raktai yra viešai prieinami. Atakuotojas, perėmęs raktus, gali priverstinai generuoti raktų sekas ir iš specializuoto įrenginio Bluetooth ryšiu (Aplikacijos naudojamo artimo kontakto identifikavimui) paskleisti jas pasirinktoje vietovėje. Ši ataka įgalina sergančiųjų skaičiaus iškreipimą – leidžia atakuotojui dauginti diagnozės raktus (identifikatorius), juos transliuoti Bluetooth ryšiu taip sukuriant fiktyvius židinius.
2. Vartotojo anonimiškumo atskleidimas. Atakuotojas gali vykdyti ilgalaikę mob. įrenginių siunčiamų Bluetooth identifikatorių registraciją, tikslinį jų saugojimą įsimenant geolokacijos vietą. Vartotojui patvirtinus COVID-19 ligą ir paviešinus jo raktą, atakuotojas iš surinktų Bluetooth trakto stebėjimo duomenų gali identifikuoti vartotoją, išaiškinti jo judėjimo maršrutus.
3. „Android OS“ skirta „Korona Stop LT“ aplikacija nėra atspari Man-in-the-Middle atakoms. Šios atakos metu atakuotojas turi galimybę perimti vartotojo į serverį siunčiamą informaciją ar ją modifikuoti vartotojui nežinant. Yra žinoma, kad asmeniniai vartotojo duomenys tinklo traktu nesiunčiami, todėl šios atakos metu tokio pobūdžio duomenų nutekėjimo rizikos nėra. Panaudojus šią ataką prieš mob. įrenginį galima perimti ir sustabdyti ligos rakto siuntimą serveriui. Tokiu atveju, diagnozės raktas sistemoje gali būti neužregistruotas.
4. Sistemos veikimas yra imlus mob. įrenginio skaičiavimo resursams. Sistemos darbo principas – sergančiųjų vartotojų raktų mainai ir jų apdorojimas. Į mob. įrenginį iš serverio periodiškai yra atsiunčiami sergančiųjų vartotojų raktai, kurie įrenginyje turi būti apdorojami turimais skaičiavimo resursais. Skaičiavimo resursų imlumo pasekmė – įrenginys informacijos apdorojimo metu atlieka daug operacijų, kurių metu apkraunami turimi aparatiniai resursai. Dėl to iš dalies mažėja įrenginio stabilumas, eikvojamas įrenginio akumuliatorius. Sistemai dirbant įprastu režimu ir apdorojant sergančiųjų Lietuvoje skaičius, apkrovos poveikis šiuolaikiniuose mob. įrenginiuose bus minimalus. Tačiau verta pažymėti, kad „KoronaStopLT“ aplikaciją integravus į bendrą sistemą visai Europos Sąjungai, mob. įrenginiuose bus tikrinami visi sistemoje esantys diagnozės (ligonių) raktai. Tai potencialiai kelia riziką stabiliam mob. įrenginių veikimui, gali stipriai padidinti akumuliatoriaus išsikrovimą.

Pažymime, kad išvardytų atakų realizavimui būtina specializuota įranga, ekspertinės kibernetinio saugumo žinios, tinkamai suprojektuota ir įgyvendinta infrastruktūra. Galima pagrįstai vertinti, kad pažymėtas atakas sudėtinga įgyvendinti praktikoje, tačiau viešai prieinama protokolo „Exposure Notifications“ dokumentacija, atviros protokolo kūrėjų elektroninės diskusijų erdvės, santykinai jaunas technologijos amžius sudaro sąlygas naujų spragų atradimams, lemiant kibernetinių rizikų fono augimą.

Sprendimo aprašuose nėra konkrečios informacijos apie planuojamą naudoti infrastruktūrą – parinktą aparatūrą ar programinę bazę, infrastruktūros išdėstymą, realizuotus saugumo ir patikimumo sprendimus, nėra pateikta informacijos apie atliktus saugumo auditus. Nors tai nėra tikslinis „KoronaStopLT“ programinio sprendimo tyrimo objektas, tačiau dėl esančio poreikio sistemai atitikti aukštus kibernetinio saugumo reikalavimus, tikslinga įvertinti ir paminėtas sprendimo dedamąsias.

Atlikus „KoronaStopLT“ aplikacijos kodo lyginamąją analizę su rinkoje esamais sprendimais nustatyta, kad „KoronaStopLT“ aplikacija itin stipriai paremta nemokamu viešai prieinamu atviro kodo projektu „Corona-Warn-App“. Tai Vokietijoje sukurtas produktas, išleistas atviro kodo formatu. Produktą kūrė įmonės „SAP“ ir „Deutsche Telekom“, projekto biudžetas – 20 mln. Eur., pirmosios

versijos išleidimo data – 2020 m. birželio 16 d., projektas pasiekiamas internetiniu adresu – *https://github.com/corona-warn-app*.

Nustatyta, kad „Android OS“ sistemai skirtos „KoronaStopLT“ aplikacijos kodo sutapimas su „Corona-Warn-App“ aplikacija yra 92,74%. „iOS“ sistemai skirtos „KoronaStopLT“ aplikacijos kodo sutapimas su vokiška aplikacija – 98%, serverio sutapimas – 99,56%. Dėl itin stipraus „Corona-Warn-App“ bazės naudojimo „KoronaStopLT“ sprendime būtina atsižvelgti į originalaus produkto kūrėjų rekomendacijas infrastruktūrai, mob. įrenginiams, sistemos konfigūracijai. Svarbu sekti ir laiku realizuoti saugumą užtikrinančius pakeitimus, diegti programinius atnaujinimus visoje „KoronaStopLT“ infrastruktūroje. Siekiant užtikrinti aukštą sprendimo kibernetinio patikimumo lygį, NKSC rekomenduoja periodiškai vykdyti „KoronaStopLT“ saugumo auditą visos sistemos apimtyje.

REKOMENDACIJOS

1. Sprendimo aprašuose nėra konkrečios informacijos apie planuojamą naudoti infrastruktūrą – parinktą aparatūrą ar programinę bazę, infrastruktūros išdėstymą, realizuotus saugumo ir patikimumo sprendimus, nėra pateikta informacijos apie atliktus saugumo auditus. Nors tai nėra tikslinis „KoronaStopLT“ programinio sprendimo tyrimo objektas, tačiau dėl esančio poreikio sistemai atitikti aukštus kibernetinio saugumo reikalavimus, tikslinga įvertinti ir paminėtas sprendimo dedamąsias.
2. Sprendime nėra numatyti aiškūs sistemos apsaugos mechanizmai. Šiuos mechanizmus būtina numatyti ir realizuoti technologinėmis priemonėmis: įdiegti ugniasienių sprendimus (kurie blokuotų žinomus kenksmingus IP adresus), apriboti užklausų per sekundę kiekį (siekiant išvengti per didelės apkrovos), servisų komunikacija tarpusavyje apsaugoti TLS v1.2 arba TLS v1.3 transporto kanalais pritaikant „Mutual Authentication“ technologiją.
3. Kadangi buvo nustatyta, kad „KoronaStopLT“ aplikacija itin stipriai paremta projekto „Corona-Warn-App“ techniniais sprendimais, rekomenduojama „KoronaStopLT“ vystytojui realizuoti infrastruktūrą operatyviam aktualių saugumo korekcijų perkėlimui iš „Corona-Warn-App“ į „KoronaStopLT“ sistemą.
4. Rekomenduojama „KoronaStopLT“ vystytojui užtikrinti produkto pokyčių vystymo, testavimo ir realizavimo aplinką, periodiškai vykdyti „KoronaStopLT“ saugumo auditą visos sistemos apimtyje.