PENETRASJONSTEST SMITTESTOPP

SAMMENDRAG

18. DESEMBER 2020

INNHOLD

1 SAMMENDRAG

BDO har på oppdrag fra Norsk Helsenett SF utført en penetrasjonstest av mobilappen Smittestopp. Smittestopp er en app fra Folkehelseinstituttet (FHI). Den skal bidra til å forhindre at koronaviruset sprer seg i samfunnet, og er helt frivillig å bruke. Appen har 16-års aldersgrense. Hensikten med penetrasjonstesten var å teste appen og tilhørende API-er mot misbruk og verifisere at beste sikkerhetspraksis for slike tjenester er oppfylt.

1.1 OPPSUMMERING AV DE VIKTIGSTE FUNNENE

POSITIVT	Pålogging til appen krever sikker autentisering med ID-porten. Det ble ikke funnet svakheter i autentiseringsflyten.
POSITIVT	Det lyktes ikke å injisere noe ondsinnet kode i appen eller gjennom API-ene.
POSITIVT	Personvern for brukerne er godt ivaretatt gjennom personvernerklæring og sikker lagring av personsensitive data.

1.2 IMPLEMENTERTE TILTAK UNDERVEIS I PENETRASJONSTESTEN

- Cookie for lastbalanserer er deaktivert på Backend-server, da denne ikke var i bruk.
- Støtte for TLS1.0/1.1 deaktivert på vl-op.ss2.fhi.no
- Tiltak mot forfalsking av e-post er implementert på smittestopp.no.
- Omdirigering fra smittestopp.no til helsenorge.no/smittestopp

1.3 BAKGRUNN

Folkehelseinstituttet har valgt den danske leverandøren Netcompany til å utvikle en norsk versjon av den danske smittesporingsappen.[1] Kildekode for appen er åpent publisert på GitHub.[2]

Smittestopp benytter rammeverket GAEN[3] for kontaktsporing. Google/Apple Exposure Notification har innebygget personvern ved at posisjonsdata lagres distribuert hos hver enkelt bruker i stedet for å samles inn til et sentralt system.[4]

Det er behov for å sikre at Smittestopp ikke kan misbrukes til å ramme enkeltpersoner som bruker appen eller til å påvirke helseberedskapen negativt. Mobilappen kan lastes ned og analyseres av personer med kriminelle hensikter. I tillegg er kildekode og API eksponert på Internett og dermed potensielt utsatt for angrepsforsøk. Et vellykket datainnbrudd kan føre til tap eller endring av sensitive data, samt forårsake nedetid. Det er også en risiko for at informasjonslekkasjer fra API kan utnyttes til å angripe andre tjenester.

Historiske tilfeller av sikkerhetsbrudd i tilknytning til mobilapper har bl.a. vært at:

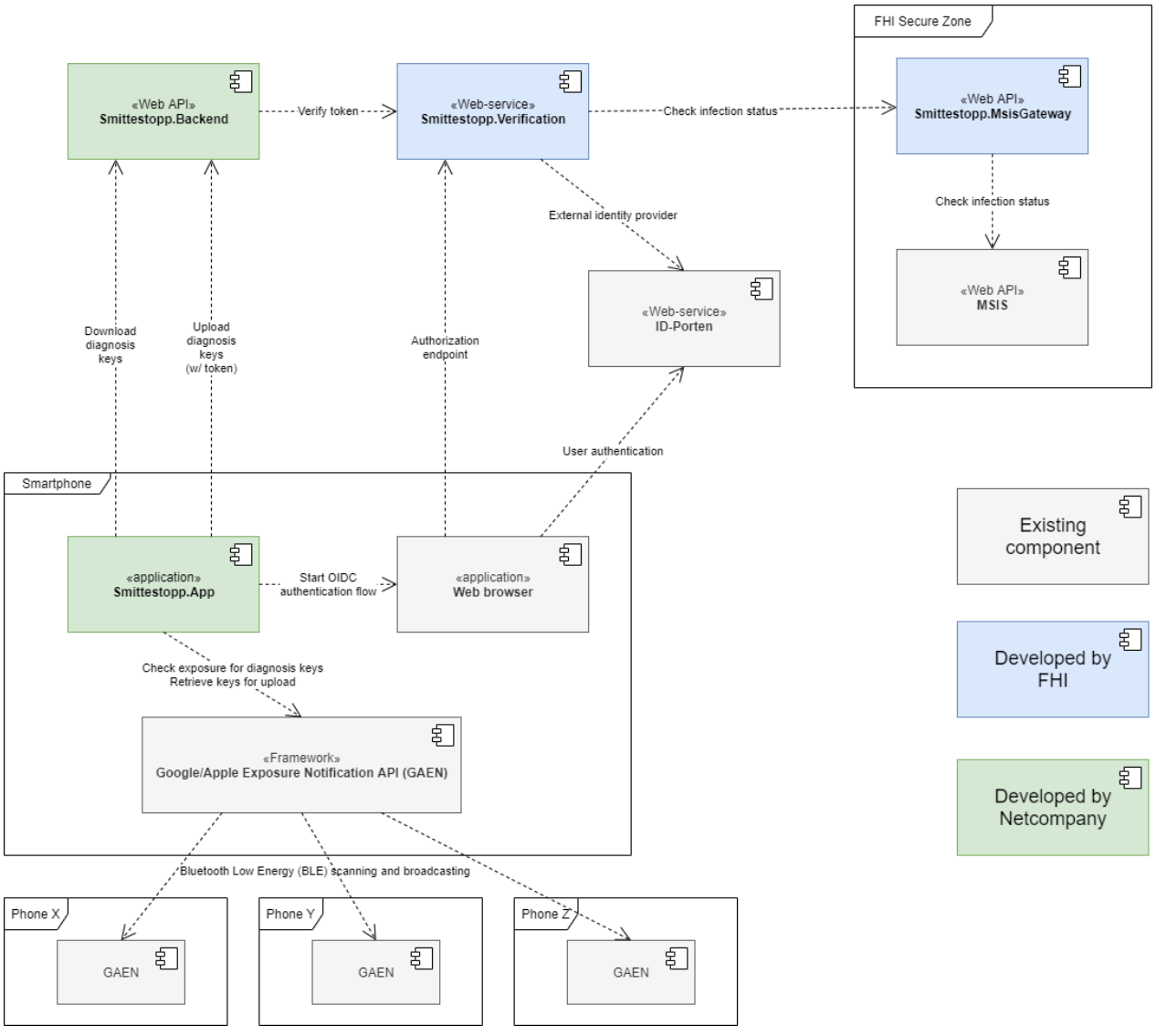
- Kommunikasjon mellom mobilapp og server-API er ukryptert eller sårbart for man-in-the-middle-angrep slik at uvedkommende kan avlese sensitiv informasjon eller manipulere data.
- Mobilapp lagrer passord, autentiseringsnøkler eller annen sensitiv informasjon ubeskyttet på en slik måte at uvedkommende kan få tilgang til enkeltbrukeres konto eller i verste fall hele brukerdatabasen.
- Server-API inneholder endepunkter som ikke krever autentisering eller mangler inputvalidering, slik at det er mulig å hente ut sensitiv informasjon om andre brukere.

[1] https://www.netcompany.com/no/Nyheter/Netcompany-utvikler-ny-smittestopp-app-i-Norge
[2] https://github.com/folkehelseinstituttet/Fhi.Smittestopp.Documentation
[3] https://en.wikipedia.org/wiki/Exposure_Notification
[4] https://smittestop.dk/uploads/konsekvensanalyse_vedr_databeskyttelse.pdf

1.4 SCOPE

Følgende komponenter inngikk i penetrasjonstesten:

- Smittestopp.App (beta)
  - Version 1.0 Build 31 for Android
  - Version 1.0 Build 50 for iOS
  - https://github.com/folkehelseinstituttet/Fhi.Smittestopp.App
- Smittestopp.Backend
  - Preprod: qa-be-op.ss2np.fhi.no (62.242.35.53, INTERXION-NET, DK)
  - Prod: be-op.ss2.fhi.no (62.242.35.52, INTERXION-NET, DK)
  - https://github.com/folkehelseinstituttet/Fhi.Smittestopp.Backend
  - https://be-op.ss2.fhi.no/index.html (Swagger)
- Smittestopp.Verification
  - Preprod: qa-vl-op.ss2np.fhi.no (83.118.185.112, NO-NHN-20031216, NO)
  - Prod: vl-op.ss2.fhi.no (83.118.185.131, NO-NHN-20031216, NO)
  - Prod – passiv backup: osl-vl-op.ss2.fhi.no (83.118.188.81, NO-NHN-20031216, NO)
  - https://github.com/folkehelseinstituttet/Fhi.Smittestopp.Verification



Figur 1 – Arkitekturskisse. Kilde: https://github.com/folkehelseinstituttet/Fhi.Smittestopp.Documentation

Smittestopp.Backend er utviklet og driftet av Netcompany.

Smittestopp.Verification er utviklet av Folkehelseinstituttet og driftet av Norsk Helsenett.

Smittestopp.MsisGateway er en intern komponent utviklet av Folkehelseinstituttet. Denne er ikke direkte eksponert og inngår ikke i penetrasjonstesten av mobilappen.

Mobilappens API-integrasjon mot MSIS, ID-porten og GAEN er testet som en del av applikasjonsflyten, men utover dette er disse eksterne komponentene utenfor scope for penetrasjonstest av Smittestopp.

Mobilapp for Android og iOS ble penetrasjonstestet opp mot OWASP Mobile Top 10.[5] Testingen ble utført både i emulator og på fysiske enheter (Android/iOS). Kildekode ble gjennomgått i forkant av penetrasjonstest og i forbindelse med dynamisk testing av mobilappen.

Testbrukere for ID-porten[6] ble benyttet.

Backend og Verification ble sårbarhetsskannet med Nessus Professional[7] og Acunetix[8].

1.5 TESTCASER

Tabellen under oppsummerer testcasene som ble brukt (OWASP Mobile Top 10).

Nr	Testcase	Sårbarhet
M1	Usikker bruk av plattform	INGEN
M2	Datalagring	INGEN
M3	Kommunikasjon	INGEN
M4	Autentisering	INGEN
M5	Kryptering	INGEN
M6	Rettighetsstyring	INGEN
M7	Klientkodekvalitet	INGEN
M8	Kodemanipulering	INGEN
M9	Reverse engineering	INGEN
M10	Skjult funksjonalitet	INGEN

1.6 TIDSPLAN

- 16. november – Oppstartsmøte og gjennomgang av løsningen med NHN, FHI og Netcompany
- 17. november – All kildekode publisert offentlig på GitHub
- 18. november – 4. desember – Kildekodegjennomgang og forberedelser til penetrasjonstest
- 7. desember – 11. desember – Penetrasjonstest av mobilapp mot preproduksjonsmiljø
- 18. desember – Sårbarhetsskanning av produksjonsservere for Backend og Verification

[5] https://owasp.org/www-project-mobile-top-10/
[6] https://difi.github.io/felleslosninger/idporten_testbrukere.html
[7] https://www.tenable.com/products/nessus/nessus-professional
[8] https://www.acunetix.com/vulnerability-scanner/

1.7 VURDERING AV KRITIKALITET

Rapporten benytter følgende skala for å vurdere sårbarheters kritikalitet.

HØY	Det er avdekket sårbarheter som er utnyttet, og det er oppnådd full kompromittering.
MEDIUM	Det er avdekket sårbarheter som potensielt kan utnyttes som steg på veien til full kompromittering.
LAV	Det er avdekket avvik fra god praksis eller sårbarheter som kan gjøre det lettere å gjennomføre målrettede dataangrep.
INGEN	Det er ikke identifisert noen avvik fra god praksis eller behov for tiltak.

1.8 AVGRENSNINGER OG FORBEHOLD

Under en sikkerhetstest av IT-systemer prioriteres det alltid å bruke tid på angrepsvektorer som utnyttes av kjente trusselaktører. Selv om grundig sikkerhetstesting utføres etter beste praksis, er det alltid en risiko for at systemet inneholder ukjente sårbarheter som ikke blir avdekket.

Testingen ble utført i et kost/nytte-perspektiv, gitt tiden som var til rådighet. Penetrasjonstesten ble utført som en «white box»-test, hvor testerne hadde tilgang til kildekode. Det ble ikke gjennomført en fullstendig kildekodegjennomgang, men kildekoden ble gjennomgått for å understøtte penetrasjonstesten. Det ble derfor fokusert på de kritiske delene av koden med tanke på mulige sikkerhetsbrudd.

Sosial manipulasjon og *tjenestenekt* er kjente teknikker potensielt brukt av kriminelle, men har ikke blitt benyttet i gjennomføringen. Førstnevnte er primært en ikke-teknisk tilnærming som trusselaktører kan bruke som delmål for å tilegne seg uautorisert tilgang til et system, mens sistnevnte er en teknisk tilnærming som trusselaktører kan benytte til å forårsake driftsavbrudd.

Rapporten oppsummerer funn som anses relevante, slik at systemeier kan vurdere risikoreduserende tiltak. Det anbefales at relevant(e) driftsleverandør(er) gjøres kjent med detaljene i rapporten, slik at de enkelte funn kan bekreftes og eventuelle sårbarheter relatert til disse lukkes.

BDO AS tar ikke ansvar for resultatet av beslutninger som fattes basert på rapporten. Rapporten er ikke å regne som en godkjenning eller sertifisering av systemet som ble testet. Oppdraget ble utført av BDOs underleverandør DEFENDABLE AS, nå utskilt fra BDO og tidligere kjent som BDO Cybersecurity.

KONTAKT

cybersecurity@bdo.no