Rahmenbedingungen (Scope) und Regeln (Rules of Engagement) des Public Security Tests

Rahmenbedingungen und Regeln sind nur in englisch verfügbar.

Regarding the Public Security Test (PST) of the SwissCovid Proximity Tracing System

Introduction

- The goal of the Public Security Test (PST) is to validate the security and to build trust in the SwissCovid Proximity Tracing System before the public rollout.
- The Swiss Federation wants to be as transparent as possible about the functioning and the security of the Proximity Tracing System. This is why all components are open source and a public security test is performed.
- The National Cyber Security Centre (NCSC) is the single point of contact (SPOC) when challenging the SwissCovid Proximity Tracing System.
- The scope of the PST is strictly limited to the dedicated Swiss Proximity Tracing System. Any other services and infrastructures are off-limits.
- By participating in the PST, you agree to be bound to these Rules of Engagement.

Organization of the PST

- The PST is time-limited in order to enable the public rollout. It starts 28.05.2020. The NCSC will end on its own decision, taken depending on the amount of findings over time.. However, submissions will also be reviewed later, in order to continuously improve the proximity tracing system also in the future, for such submissions, the same rules apply.
- There is no registration required or possible for the PST.
- There is no compensation for participating in the PST and/or for submitting findings.
- NCSC serves as single point of contact for all participants. NCSC is mainly responsible for issue management, classification of findings and any queries you have regarding the PST.

Testing policy

- The Swiss Confederation provides a proximity tracing system dedicated to fight the Covid-19 pandemic. All participants have access to the proximity tracing test system. All interactions with the system will be logged. Such logs will be deleted 30 days after the PST is finished.
- Participants are permitted to perform any tests and investigations on the dedicated proximity tracing test

system as long as they act in good faith and respect the scope of the test provisions (see below).
- Participants who have found or believe they have found a vulnerability are asked to submit a report via following NCSC Website: https://www.melani.admin.ch/melani/en/home/public-security-test/reporting_form.html (https://www.melani.admin.ch/melani/en/home/public-security-test/reporting_form.html)

Scope of the test

- The scope of the PST is a security test of the proximity tracing system. It contains the mobile app (iOS/Android) and the backend of the proximity tracing system. The following core components are all open sourced and can be found in the following repositories:
  Android repository:
  https://github.com/DP-3T/dp3t-app-android-ch
  (https://github.com/DP-3T/dp3t-app-android-ch)
  iOS repository:
  https://github.com/DP-3T/dp3t-app-ios-ch
  (https://github.com/DP-3T/dp3t-app-ios-ch)
  Covidcode Frontend:
  https://github.com/admin-ch/CovidCode-UI
  (https://github.com/admin-ch/CovidCode-UI)
  App backend:
  https://github.com/DP-3T/dp3t-sdk-backend
  (https://github.com/DP-3T/dp3t-sdk-backend)
  App config backend:
  https://github.com/DP-3T/dp3t-config-backend-ch
  (https://github.com/DP-3T/dp3t-config-backend-ch)
  Covidcode backend:
  https://github.com/admin-ch/CovidCode-Service
  (https://github.com/admin-ch/CovidCode-Service)
- Any systems that are not clearly identifiable as part of the dedicated proximity tracing test system are not in-scope. If you are unsure, then please stop your activity and ask NCSC first.
- Attacks and scans that can harm other operations and services of the Swiss Confederation, ETH or EPFL are not in-scope and are therefore strictly forbidden. If you are unsure, then please stop your activity and ask NCSC first.

Out-of-scope

Everything that is not defined as in-scope is out-of-scope by default. In particular, the following items are out-of-scope:

- All attacks that fall in the broad denial of service (DDoS) and resource starvation categories.
- Social engineering, phishing or malware attacks on operators or employees of the Swiss Confederation, ETH, EPFL or the Cantons.
- Physical attacks on people, buildings and devices.
- Attacks on the (GitHub) code repositories or the report submission website of NCSC
- Lateral movements after a compromise of a system.

If you are unsure, then please ask NCSC first: https://www.melani.admin.ch/melani/de/home/kontakt.html (https://www.melani.admin.ch/melani/de/home/kontakt.html)

Submission Guidelines

- Submissions of vulnerabilities need to be done via respective form on the NCSC website: https://www.melani.admin.ch/melani/en/home/public-security-test/reporting_form.html
  (https://www.melani.admin.ch/melani/en/home/public-security-test/reporting_form.html)
- Submissions to other parties or through other channels will not be reviewed and will therefore not contribute to the PST.
- Submissions must contain:

  A basic description of the issue in question

  Affected components (e.g. Android App, Backend, etc.)

  A step-by-step reproduction guide of the finding

  A tentative risk-classification of the issue

  Submissions ideally contain: accompanying evidence, e.g. screenshots, videos, proof of concept code, dumps, etc.

  If you upload attachments, please provide either pure ASCII text (e.g. Markdown) or PDF-A.

  If possible: Please provide a mean of contacting you in case of any questions from the developers, If you have a PGP key or S/MIME certificate, you may want to provide that as well in order to communicate securely.

Responsible disclosure policy

- Already submitted findings are published on NCSC's website on a daily basis for transparency reasons: https://www.melani.admin.ch/melani/en/home/public-security-test/current_findings.html
  (https://www.melani.admin.ch/melani/en/home/public-security-test/current_findings.html)
- Participants are allowed to publish their findings after the respective finding is published on NCSC's website.
- When findings are published on NCSC's website, the original reporter of the finding will be credited if the reporter agrees to such publication. It is possible to request to remain anonymous or to use a pseudonym.

Consequences of complying with the Rules of Engagement

The Swiss Confederation, represented by the NCSC

- Interprets activities by participants that comply with the Rules of Engagement as authorized access under the Swiss Penal Code. This includes Swiss Penal Code paragraphs 143, 143bis and 144bis.
- Will not take civil action or file a complaint with law enforcement authorities against participants for accidental, good faith violations of the Rules of Engagement.
- Will not file a complaint against participants for trying to circumvent the security measures deployed in order to protect the proximity tracing test system in-scope as outlined above.
- For breaches of the Rules of Engagement, the Swiss Confederation reserves the right to file criminal charges.

Applicable law and jurisdiction

The Rules of Engagements are governed by and construed in accordance with the laws of Switzerland.

Berne, 26th May 2020

✉ Fachkontakt
(mailto:incidents@ncsc.ch)

Letzte Änderung 18.06.2020