Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Chancellery FCh

Release of source code leads to discovery of flaw in Swiss Post's new e-voting system

Bern, 12.03.2019 - Researchers have uncovered a significant flaw in the new e-voting system of Swiss Post. The flaw concerns the system offering universal verifiability, which is currently undergoing a public intrusion test. It does not affect the system already being used in four cantons. The flaw does not allow the system to be intruded. The Federal Chancellery has urged Swiss Post to take appropriate measures to prevent such flaws.

In the course of the public intrusion test in conjecture with the publication of the system's source code, testers uncovered on March 12th, 2019 what the Federal Chancellery considers to be a significant flaw in the new e-voting system of Swiss Post. They came across the flaw by studying the system's source code and the accompanying documentation, and subsequently notified the Federal Chancellery and Swiss Post. The public intrusion test, which involves the release of the source code, is intended to reveal possible vulnerabilities so that they can remedied.

The flaw identified concerns the implementation of universal verifiability. Verifiability is a way of determining by means of mathematical proofs whether votes have been manipulated. While the flaw does not allow the system to be penetrated, the researchers were able to demonstrate that the system does not generate conclusive mathematical proofs to identify whether any manipulation has taken place. This means that it is not possible to detect whether the votes have been tampered with. The existence of this flaw means that the system does not comply with the legal requirements set out in the Federal Chancellery Ordinance on Electronic Voting (OEV).

Federal Chancellery to review certification procedure

The Federal Chancellery has called on Swiss Post to review and improve its security processes to prevent such flaws. Swiss Post should also review and adapt the conditions for accessing the source code. The Federal Chancellery for its part will review the relevant certification

and authorization procedures.

Existing system not affected

The flaw that has come to light concerns Swiss Post's newly developed e-voting system. The existing system, for which the cantons already have an initial licence issued by the Federal Council, does not offer universal verifiability and is therefore not affected by this flaw. Ten cantons currently offer a certain proportion of the electorate in their cantons the possibility of voting electronically; four operate Swiss Post's current system.

The Federal Council and the Federal Chancellery decide whether to issue an initial licence and authorisation to use e-voting systems when a canton submits a corresponding application. They only authorise the use of systems which fulfil the requirements stipulated under federal law.

Intrusion test to continue

On 5 April 2017 the Federal Council decided that providers of universally verifiable systems would have to publish the source code. In the same year, the Confederation and the cantons also agreed that a public intrusion test would be conducted as a pilot trial. These measures are intended to generate transparency and harness the expertise of external IT specialists.

The public intrusion test on Swiss Post's system runs until 24 March, which provides time to see whether any further flaws come to light. The Confederation and the cantons will evaluate the results of the test and then publish a report. The Federal Chancellery will assess whether further corrections to the new system are needed, and whether there is a need to adapt the existing e-voting system.

Address for enquiries

René Lenzin
Dep. Head, FCh Communication Service
+41 58 462 54 93
rene.lenzin@bk.admin.ch

Links

Ergebnisse der Forscher / résultats des chercheurs /

Publisher

Federal Chancellery
http://www.bk.admin.ch/index.html?lang=en

Last modification 31.10.2017

https://www.bk.admin.ch/content/bk/en/home/dokumentation/medienmitteilungen.msg-id-74307.html