Error in the source code discovered and rectified

12-03-2019

The public intrusion test ordered by the Confederation and the cantons on Swiss Post's e-voting system and the published source code has delivered its first valuable results. International IT experts found a critical error in the source code relating to universal verifiability. The error in itself did not make it possible to infiltrate the e-voting system. Swiss Post requested that its technology partner, Scytl, correct the error in the code immediately and they have already done so. The modified source code will be applied with the next regular release.

The public intrusion test ordered by the Confederation and the cantons on Swiss Post's e-voting system has been running for well over two weeks. More than 3,000 hackers from around the world are putting the system through its paces until 24 March. The system is one of the newest generations with universal verifiability. In addition to the intrusion test, Swiss Post published the certified source code for its e-voting system on 7 February. This was a legal requirement of the Confederation.

International IT experts found a critical gap in the source code and informed Swiss Post. The experts were able to demonstrate that the gap could be used to manipulate votes without it being able to be proven. However, the error in itself did not make it possible to infiltrate the e-voting system. To exploit the weak point the attacker had to override numerous protective measures. They needed control over Swiss Post's secured IT infrastructure, for example, as well as help from several insiders with specialist knowledge of Swiss Post or the cantons.

The error in the source code relates to universal verifiability. It was already identified in 2017. However, the correction was not made in full by the technology partner Scytl, which is responsible for the source code. Swiss Post regrets this and has asked Scytl to make the correction in full immediately, which they have done. The modified source code will be applied with the next regular release.

The e-voting system currently being used in the cantons of Thurgau, Neuchâtel, Fribourg and Basel-Stadt is not affected by this gap in the source code. It exclusively affects the system with universal verifiability provided for the intrusion test, which has never been used for a real vote.

Input from the hacker test incorporated into further development

E-voting systems need to withstand countless quality tests and simulated hacker attacks for them to be approved for real votes. Swiss Post wants a secure e-voting system and is following all the requirements and conditions set out by the Confederation and the cantons. It will incorporate the results of the hacker test and the analysis of the source code into the development of its e-voting system and put them to the test. That is the very point of a public intrusion test. The results are evaluated, ordered by degree of severity and rectified in line with the risk involved. Confirmed weaknesses will be published on the relevant platform promptly and in a transparent manner.

Source: Swiss Post