Swiss Post puts e-voting on hold after researchers uncover critical security errors

James Walker 05 April 2019 at 08:35 UTC

Election Security | Government | Cryptography

'Until we can get beyond foolish publicity stunts, e-voting will remain an insecure clusterfuck'

Swiss Post has suspended its controversial online voting (e-voting) system after a team of researchers unearthed a series of critical errors in the system's source code.

E-voting in Switzerland was thrust into the spotlight back in February, when Swiss Post announced it would open up the source code and invite hackers to test its new voting system for security vulnerabilities.

However, before the planned 'public intrusion test' had even started, the code came under the scrutiny of an international team of researchers – Sarah Jamie Lewis, Vanessa Teague, and Olivier Pereira – who discovered three critical flaws (PDF) that could lead to undetectable vote manipulation, among other shortcomings.

Choosing to eschew any financial reward promised by the e-voting bug bounty program, the researchers published the first of three white papers outlining the vulnerabilities on March 12.

"Let us not downplay this," Lewis said in Twitter thread posted on the day of the researchers' initial disclosure. "This code is intended to secure national elections.

"Election security has a direct impact on the distribution of power within a democracy. The public has a right to know everything about the design and implementation of the system."

Critical errors

Switzerland has long been ranked among the e-voting pioneers. Several cantons have been experimenting with electronic voting (PDF) since the early 2000s, and Swiss Post (the country's national postal service and the organization tasked with overseeing the nation's online voting program) has previously said it was aiming for all residents to be able to vote online in elections and referendums.

This paved the way for the public intrusion test of a new, "universally verifiable e-voting system" from Barcelona-based Scytl. The testing period, which offered financial rewards for successful vulnerability discoveries, ran from February 25 to March 24.

According to Swiss Post, more than 3,000 researchers participated in the program. Of the 173 vulnerabilities that

Latest Posts

'Why am I receiving this email?'
Agari applies behavioral analysis to BEC scams
05 April 2019

Social Security – w/e 5 Apr
'Meet the heroes who stepped up when it mattered the most'
05 April 2019

Backdoor discovered in Bootstrap-Sass Ruby library
05 April 2019

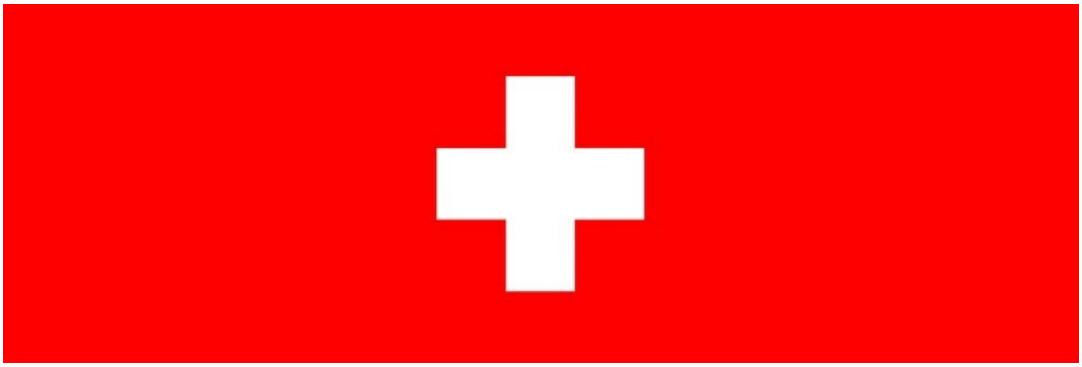
Hacker stereotypes must be broken to bridge the skills gap
04 April 2019

were submitted, 16 were confirmed as valid – although all of these flaws fell under the lowest classification level: 'Best Practice'.

This, of course, leaves the three critical vulnerabilities discovered by Lewis, Teague, and Periera. The researchers did not participate in the public intrusion test, but it was clear that their findings could not be ignored.

"Although the electronic ballot box could not be hacked, feedback on the published source code reveals critical errors," Swiss Post said in a statement last week.

"Since the integrity of votes and elections is a top priority, Swiss Post is taking action. It will correct the source code and have it reviewed again by independent experts. It will therefore not provide its e-voting system to the cantons for the votes of May 19."



Setting a precedent

Following the public intrusion test, Swiss Post and Scytl have hailed the program as something of a success.

(Scytl issued a statement on April 1 saying the scheme "set a precedent" for government-run e-voting programs. A Swiss Post spokesperson told *The Daily Swig* that the discovery of vulnerabilities was "the very point of the public intrusion test".)

Not so for Lewis who, along with several other notable cryptographers and privacy experts, remains a vocal opponent to a public intrusion test, particularly as the critical flaws in Scytl's proprietary e-voting technology were not discovered in previous audits.

"Any government that decides to entrust Scytl with their democracy after all of this should be regarded with intense suspicion [and] placed under harsh scrutiny," she wrote over the weekend.

Providing added context, Lewis told *The Daily Swig*: "We did not go through the disclosure process outlined by Swiss Post because we felt that agreeing to their NDA [non-disclosure agreement] would be unethical and not in the interest of the public, who have a right to know about critical issues in their voting systems.

"The response from Swiss Post was civil, but both they and Scytl minimized the issue. Even after our second and third disclosures we have yet to see any remorse from Scytl or Swiss Post for the statements they made about our original comments on their code base.

"I worry that they will continue to repeat the same mistakes."

A vote for the future

When asked to provide a projected future timeline for its e-voting system, Swiss Post spokeswoman Jacqueline Buehlmann told *The Daily Swig* that the organization aims to reinstate online voting in certain cantons later this year.

"Our system is used by four cantons (Fribourg, Neuchâtel, Thurgau and Basel-Stadt) at the moment," she said. "In most of these cantons, e-voting is only available for Swiss [nationals] living abroad.

"Because security is a top priority for Swiss Post, it will not make its e-voting system available to these cantons for the votes on May 19.

"The decision not to go to the polls gives Swiss Post time to carefully implement the corrections and have them checked again by independent experts. It is currently planned to offer the cantons a revised system for the federal parliamentary elections in autumn."

René Lenzin, deputy head of communication for the Swiss Chancellery, added: "This review will include the licensing and certification procedures for e-voting systems. The Confederation will authorize e-voting only if the cantons and their providers manage to meet the federal requirements."

While Lewis has welcomed Swiss Post's decision to put the brakes on its e-voting service, she expressed doubts that the developers will be able to make the necessary improvements in such a short timeframe.

"I'm happy about the suspension, but the timeline some of the cantons have provided for e-voting to resume (October 2019) seems highly unrealistic considering the current state of the code and the number of critical vulnerabilities that we found in such a short time," Lewis told *The Daily Swig*.

When asked what she feels is the best course of action for those tasked with overseeing the security of Switzerland's online voting system, Lewis urged for "a public inquiry into why so many audit mechanisms failed".

"After that, print out the source code, go through it line by line to identify any other issues and then set it on fire, and start the process all over again but with a new, open source, freely-licensed system funded by the same pot that would be used to pay a proprietary system provider that failed to provide a secure code base," she said.

Despite the controversy, Lewis did express some hope that e-voting will eventually become a feasible proposition for citizens.

"E-voting is a marvellous idea, and a path forward to true representation and frequent elections, while reducing the physical costs associated with nationwide polling days," she said. "But we need open development and adequate funding for engineering and publicly accountable auditing bodies with the skills necessary to assess such systems.

"Until we can get beyond foolish publicity stunts like the PIT [public intrusion test] and into a future of established security engineering for public infrastructure, then e-voting will remain an insecure clusterfuck."

RELATED Smartphone voting brings new security concerns

James Walker

@jaywalknet