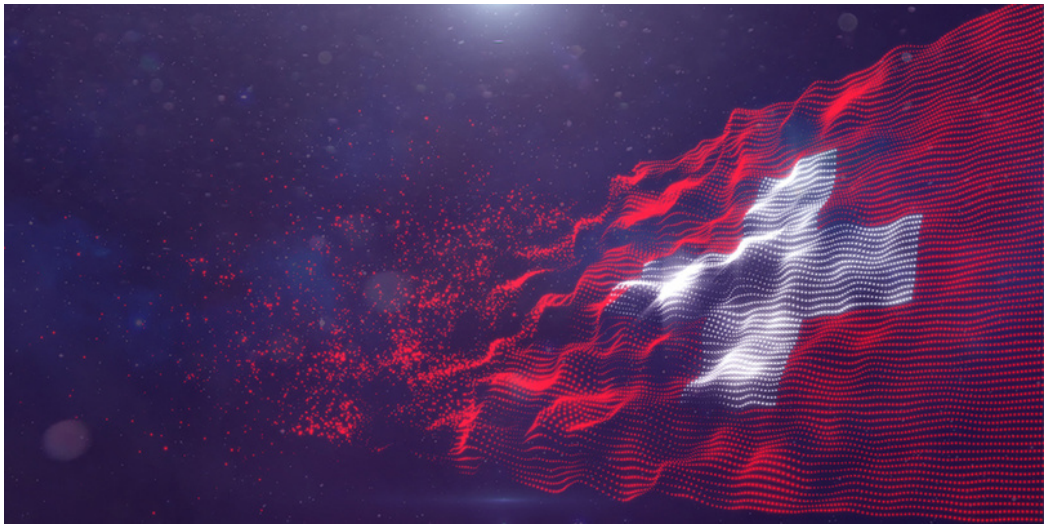
The Daily Swig
Cybersecurity news and views

E-voting intrusion test: Swiss Post bug bounty moderator tallies submissions

James Walker 11 September 2019 at 15:32 UTC

Election Security | Bug Bounty

Researchers discovered 16 'minor' vulnerabilities in controversial online voting system



Security researchers have been rewarded for their discovery of 16 low-impact vulnerabilities in an online voting (e-voting) system that's poised to be rolled out across Switzerland.

Earlier this year, Swiss Post – the country's national postal service and the organization tasked with overseeing the nation's online voting program – announced it was inviting hackers to test its e-voting system for flaws.

The 'public intrusion test' (PIT) ran from February 25 to March 24. It simulated a real federal vote, during which bug hunters could download their encrypted ballot 'cards' and scrutinize the system's open source code for vulnerabilities.

The e-voting bug bounty program offered payouts ranging from CHF100 ($100) for "uncritical optimization possibilities" to CHF50,000 ($50,000) for vulnerabilities that offered a potential mechanism to manipulate votes without being detected.

Split vote

The Swiss Post e-voting PIT was overseen by SCRT SA, a Lausanne-based IT company which last week published its final report (PDF) on the program.

According to the company, 3,186 people registered to take part in the PIT. However, of this figure, just 822 individuals requested e-voting cards.

During the program, according to SCRT, a total of 173 issues were submitted by a total of 80 participants. This was whittled down to 16 valid vulnerabilities – all of which fell into the (lowest) 'failure of best practice' category.

The vulnerabilities – which included a crafted X-Forwarded-For HTTP header injection bug, along with the discovery of vulnerable TLS cipher-suites and outdated version of the Bootstrap web framework – netted the hackers a total of just $2,000.

LISTEN NOW SwigCast, Episode 2: ENCRYPTION

Despite the seemingly low turnout figures (and even lower number of valid bugs discovered), SCRT said it was satisfied with the PIT exercise, although the company acknowledged some shortcomings.

"Overall, the PIT was a properly orchestrated 'bug bounty'," SCRT said. "The overall participation was good, and the variety of submissions suggested that the system was looked at by a large number of researchers of

Latest Posts

Apple-Corellium lawsuit raises concerns among security community
Mobile virtualization company suspec ulterior motive is behind litigation

France and India strengthen ti with cybersecurity agreement
Indo-French alliance heralds collabor on AI, 5G, and quantum computing

Cloudflare releases network scanning tool to the masses
… infosec backlash ensues

#SocialSec – w/e 22 Nov
Hot takes on this week's biggest cybersecurity news

different levels of competence."

While SCRT said the PIT seemed "properly defined and relevant", it admitted that the attack surface on "critical concepts like server-side vote secrecy or server-side vote corruption was very limited since the back-end was not directly accessible to the participants".

Also of note, said SCRT, was that the PIT's credibility "probably" suffered "from the confusion caused by the overlap with [the] source code program".

Hack early, hack often

Anyone who has been keeping track of Switzerland's e-voting program will be well aware of the controversy that emerged in the wake of Swiss Post's bug bounty announcement earlier this year.

Before the planned intrusion test had even started, the system's source code came under the scrutiny of an international team of researchers – Sarah Jamie Lewis, Vanessa Teague, and Olivier Pereira – who discovered three critical flaws 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 at the time. "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."

Swiss Post temporarily suspended its e-voting system following the researchers' disclosure.

Trial operations

With the dust now settling on the PIT exercise, Swiss Post spokesperson Jacqueline Buehlmann discussed the future of e-voting in Switzerland.

"Swiss Post has corrected the errors that national and international researchers discovered in the source code," Buehlmann told *The Daily Swig*.

"We will publish a corrected version of the source code. Specialists can then check the corrections.

"We plan to make the system with universal verifiability available to the cantons [Swiss regions] for trial operation from 2020. The cantons decide if and when they want to make e-voting available to their citizens."

E-voting remains a contentious subject for those in the security community and beyond.

Those in favor of the technology say that online ballots can help increase voter 'turnout', particularly among younger citizens, while reducing costs associated with local and national polling days.

For many others, however, there's still a long way to go until we can trust the integrity of e-voting systems.

"We're not just worried about altering the vote," cryptographer Bruce Schneier said last year.

"Sometimes causing widespread failures, or even just sowing mistrust in the system, is enough. And an election whose results are not trusted or believed is a failed election."

YOU MIGHT ALSO LIKE Incoming! Swiss CERT warns ransomware fiends are targeting local SMEs

Election Security | Bug Bounty

James Walker

@jaywalknet