Final report on the e-voting public intrusion test
17.06.2024 – 03.07.2024

Contents

1. Management summary

Swiss Post conducted a public intrusion test (PIT) on its electronic voting (e-voting) system with complete verifiability. This type of testing is also known as a penetration test or "pentest" for short in specialist circles. The implementation of repeated public intrusion tests is a legal requirement of the Swiss Confederation for e-voting trial operations.[1]

From 17 June to 3 July 2024, ethical hackers had the opportunity to conduct attacks on Swiss Post's e-voting system infrastructure. The participants tested an exact copy of the e-voting system's production environment for security vulnerabilities. The same framework conditions applied as for the real use of e-voting in elections and votes. The experts were able to simulate the vote casting process 1:1 on the voting portal using sample voting cards and target the system.

The test attracted strong interest on the professional scene: there were around 9,500 attacks on the system from 6,923 IP addresses. More than 50 attempts at access were made from 146 IP addresses. These are referred to in this report as the "most active participants".
No-one managed to penetrate the system. Swiss Post received four findings and confirmed one with low severity after testing. The finding did not concern any security-related aspects. It shows an improvement in the communication between the servers, making simultaneous requests impossible. Swiss Post has implemented the improvement in the voting server. The hacker received a reward of 1,500 francs. As the first hacker to report a confirmed finding, he also received a bonus of 3,000 francs.

---

[1] Federal Chancellery Ordinance on Electronic Voting (OEV) of 25 May 2022, Article 10

2. Introduction

As part of its cybersecurity strategy, Swiss Post publicly allows ethical hackers to attack its IT systems. The company provides financial rewards for confirmed vulnerabilities as part of bug bounty programmes. Swiss Post's experience shows that this is an extremely effective method for continually improving systems and protecting against attacks.

The Confederation's legal basis stipulates that the source code of an e-voting system must be disclosed on a permanent basis. Attacks on the infrastructure are also to be made possible in a permanent programme or as part of a recurring test with a limited duration.

Swiss Post has implemented these requirements since 2021 and offers experts the following options for testing its system:

Unlimited duration
As part of a community programme, Swiss Post has disclosed all of the main components and documents of its e-voting system with complete verifiability on an ongoing basis. Since 2021, cryptographers and hackers have been able to check the source code and system documentation for errors, simulate attacks and report findings. Experts have different testing options:

- Static tests: Search for errors and vulnerabilities in the published documents and in the source code for the e-voting software. All disclosed components are part of this test.
- Dynamic tests: experts can run the executable system on their own platform and thus find errors in the e-voting system, including back-end systems that cannot be reached directly.

Regular implementation with limited duration
With the public intrusion test, Swiss Post provides another recurring test option: ethical hackers can test an exact copy of the e-voting system's production environment for security vulnerabilities. The same framework conditions apply to the test as to the use of e-voting in elections and votes. Following the 2022 and 2023 intrusion tests, Swiss Post's fully verifiable e-voting system was put to the test for the third time in a public intrusion test from 17 June to 3 July 2024.

This report summarizes the findings of the 2024 public intrusion test.

3. Implementation of the PIT

3.1. Code of conduct
Swiss Post has defined rules of conduct for participation in its community programme (code of conduct): the code of conduct governs access to the components and documents of Swiss Post's e-voting system. These specifications are available online (https://evoting-community.post.ch/en/code-of-conduct).

In addition, the rules for participation in the public bug bounty programme apply to e-voting. These can also be viewed online (https://yeswehack.com/programs/swiss-post-evoting).

3.2. Organization
Swiss Post runs its bug bounty programmes in conjunction with the independent company YesWeHack. The YesWeHack platform is the access point to the bug bounty programme and platform via which ethical hackers can report findings if they wish to apply for a reward. After initial triage of the reports from the team at YesWeHack, a specialist Swiss Post team analyses the findings.

3.3. Scope of testing
Part of the public intrusion test was an exact copy of the e-voting system's production environment, referred to in this report as "infrastructure". This means that the test takes place under the same conditions as when e-voting is used in votes and elections.

3.4. Preparation of an electronic ballot
In the run-up to a real contest, the cantons create the electronic ballot boxes and generate a voting card for all eligible voters. As an integrated provider, Swiss Post provides the infrastructure of the e-voting system with the control components and the voting portal. This separation of competencies between the cantons and Swiss Post in the preparation of the electronic ballot is a security measure and a legal requirement of the Confederation.

Swiss Post handles all the preparatory work for a public intrusion test and provides ethical hackers with generalized sample voting cards with individual codes but without an individual identification feature (the year of birth or date of birth, depending on the canton).

The electronic ballot for the public intrusion test was defined as follows:
* A fictitious vote with two questions
* A fictitious proportional ballot with 3 lists, 4 candidates and 2 seats that can be filled fictitiously.
* A fictitious majority ballot with 5 candidates and 2 seats that can be filled fictitiously.

Swiss Post provided 5,000 sample voting cards. The sample voting cards can be downloaded without prior registration from a website.

3.5. Communication
Swiss Post provides experts and the general public with regular information about the ongoing development of the system and feedback from the community. The company publishes the confirmed findings on the specialist platform GitLab and communicates them as follows:

Overview of published information on findings from the public e-voting bug bounty programme:
- Results from the private bug bounty programme, 1 September 2021
- Results from the bug bounty programme, update 31 December 2021
- Results from the bug bounty programme, update 31 March 2022
- Results from the bug bounty programme, update 30 June 2022
- Results from the bug bounty programme, update 28 September 2022
- Results from the bug bounty programme, update 31 December 2022
- Results from the bug bounty programme, update 31 March 2023
- Results from the bug bounty programme, update 30 June 2023
- Results from the bug bounty programme, update 22 September 2023
- Results from the bug bounty programme, update 31 December 2023
- Results from the bug bounty programme, update 31 March 2024
- Results from the bug bounty programme, update 30 June 2024

Swiss Post classifies findings of the community programme into four levels of severity (low, medium, high, critical). Swiss Post describes all findings with a high or critical severity level on the specialist platform GitLab and, for a wider audience, on its e-government blog.

Swiss Post publicized the public intrusion test through various channels at the time it was launched and as it progressed:

- 07.03.2024: Save-the-date for the public intrusion test via a mailing to the e-voting specialist community (publicized by an online specialist magazine)
- 30.05.2024: Direct message (announcement) via the bug bounty platform to researchers known to Swiss Post
- 12.06.2024: Information about the start of the public intrusion test to ethical hackers who follow the bug bounty programme on the platform with the policy update on the bug bounty platform
- 17.06.2024: Information about the start of the public intrusion test to the public with an article on Swiss Post's e-government blog and news sent to a defined circle of interested media, information e-mail to the specialist community and institutional stakeholders, posts on the LinkedIn accounts of Swiss Post and on the X and LinkedIn accounts of Swiss Post's partner for the bug bounty programme.
- 26.06.2024: Posts on the X and LinkedIn accounts for both Swiss Post and the bug bounty programme partner concerning a bonus of 3,000 francs in addition to the regular rewards and information on the first confirmed finding
- 25.07.2024: Article on the Swiss Post e-government blog about the results of the public intrusion test

3.6. Conditions of participation

No registration is required to take part in the public intrusion test. Registration is required only if someone wishes to submit a finding via the YesWeHack bug bounty platform to receive a reward. All contact details remain with YesWeHack and are not forwarded to Swiss Post. The key figures on activity in the public intrusion test can be found in the section IP addresses by country.

4. Results

For the public intrusion test (scope infrastructure of the bug bounty programme), Swiss Post classified the findings using the CVSS (common vulnerability scoring system) standard scale. This scale is based on a common standard for the categorization of security findings.

In total, Swiss Post received four reports of findings. After the analysis, it was able to confirm one finding with a "low" severity. Two other findings were not confirmed and were closed as "reports". One finding was rejected (out of scope).

Swiss Post also received the following contributions during the duration of the public intrusion test:
– Four reports on the source code were received. None of these could be confirmed as findings. They were closed as reports.
– Various suggestions and questions about the e-voting community programme were received.

4.1. Findings

The confirmed finding shows an improvement in the voting server when processing simultaneous, but inconsistent requests.

Title	Simultaneous processing of different encrypted votes for the same voting card ID may lead to an inconsistent system state for that particular voting card ID.
Classification	Low
Number	#YWH-PGM2323-210
Date of receipt	17.06.2024
Reported by	Daniele Ligorio
Description	By performing multiple simultaneous sendVote attempts, it is possible to induce an inconsistent state in the system for a particular voting card ID, assuming the attacker knows the start voting key and extended authentication factor of the voter.
	Normally, the voting server receives an encrypted vote for a specific voting card ID and relays it to the four online control components. To ensure availability, the voting server handles multiple requests in parallel. The issue highlighted involves an attacker sending multiple, different requests for the same voting card ID at the same time. Due to parallel processing, different requests might be forwarded to different control components, resulting in an inconsistent state of the voting card. The current behavior leads to time-outs because the voting server fails to obtain a consistent response from the control components.
	This inconsistency does not affect the system's verifiability and voting secrecy. The problem arises from the concurrent handling in the voting server. In our threat model, the voting server is considered untrustworthy. The Swiss Post Voting System relies on at least one control component being trustworthy. The control components have robust exactly-once processing and correctly handle simultaneous requests.
	Furthermore, an attacker with the start voting key and extended authentication factor could already prevent the voter from voting electronically by submitting a vote that does not match the voter's intentions. However, the attacker cannot confirm the vote without knowing the ballot casting key, allowing the voter to still vote by mail or at a polling station.
	The voting server should handle concurrent requests more gracefully, ensuring that the same encrypted vote is forwarded to all control components.
Status	In release 1.4.3.1, we enforced that the voting server processes only one simultaneous request for a particular voting card ID and refuses any additional requests. This measure increases the robustness of the voting server and prevents any inconsistent states for a particular voting card in the system.
Reward	The person reporting the finding received a reward of CHF 1,500 plus an additional bonus of CHF 3,000, which was advertised for those submitting the first three confirmed findings.

4.2. Other findings that were not accepted

Title	Alleged missing SPF record allows email Spoofing.
Number	#YWH-PGM2323-211
Date of receipt	17.06.2024
Description	The hunter alleges, that an absence of an SPF record in your DNS configuration allows attackers to send emails that appear to originate from your domain. SPF is a widely adopted email validation system designed to detect and prevent this type of email spoofing by specifying which mail servers are permitted to send email on behalf of your domain.
Status	Closed as out-of-scope. Swiss Post sets a SPF record on the domain evoting.ch Moreover, this report cannot be considered as valid, based on our program's non-qualifying vulnerabilities. Indeed, Phishing attacks (including issues related to SPF/DKIM/DMARC) are out of scope.
Reward	None

Title	Remark regarding case-insensitivity in the start voting key and the resulting entropy of the derived key.
Number	#YWH-PGM2323-212
Date of receipt	20.06.2024
Reported by	No Breach
Description	In this report, the hunter questions whether the start voting key contains enough entropy. In particular, the hunter argues that using a case-insensitive alphabet for the Start Voting Keys (SVK) grants no particular advantage of a case-sensitive alphabet, and has a severely reduced input space compared to using a case-sensitive alphabet: A smaller input space has higher risks of obtaining two voters with the same key, which would severely break assumptions maybe about the uniqueness of the SVKs. They suggest to using case-sensitive hashing algorithms for security and collision resistance reasons.
Status	Closed as informative. Due to the extremely large size of the SVK space (32^{24}), as well as the fact that the e-voting system uses cryptographically secure functions to randomly generate these SVKs, these values are effectively guaranteed to be unique even for elections with a very large quantity of voters, and that no additional checks need to be performed by the verifier or other entities to guarantee the generation of a unique SVK value. The current alphabet was chosen intentionally for ease of use to prevent misspellings as much as possible, not to add additional characters such as symbols and/or case sensitive letters, to ensure that the SVK can be used by all citizens wishing to vote via the internet in a manner that is as easy as possible. The risk of accidentally generating the same SVKs for two voters with the same birth year is unlikely and therefore obtaining a "collision" is too small to realistically ever happen. We highlight that even if the hunter uses the term "hash collision", the scenario they describe is not related to different inputs resulting in the same hash, but two voters being given the same SVK, i.e. two same inputs (which would, as expected, obtain the same hash).
Reward	None

Title	Alleged race condition on the authentication endpoint.
Number	#YWH-PGM2323-215
Date of receipt	25.06.2024
Description	The hunter alleges that a race condition on the voting server's *authenticate* endpoint is possible and would lead to further security impacts. The hunter then describes that this behavior might lead to potential issues: • If a legitimate user authenticates to the system, an attacker could also authenticate and cast a vote before the victim. • The two users could lead the voting server to potentially be working on the same input data (e.g., the SVK_id string) and then trying to store the results in the same variable, leading to unpredictable results
Status	Closed as informative. Operations for different users operate in separate contexts in the voting server's authenticate endpoint. Therefore, we could not identify any potential race conditions. Additionally, the hunter has not provided any tangible demonstration on how such a race condition could be achieved.
Reward	None

4.3. Participants

All domains with IP addresses assigned with the pattern pit.evoting.ch were part of the scope defined for the public intrusion test. In practical terms, this means that the ethical hackers were able to attack the e-voting server using the voting portal (pit.evoting.ch), each with their own IP address.

- During the public intrusion test, the pit.evoting.ch server was accessed from around 6,923 different IP addresses via the HTTP/HTTPS protocols.
- In total, more than 50 attempts to access to the e-voting server were registered from 146 IP addresses. These are referred to as the "most active participants".

4.3.1. IP addresses by country

In total, we detected access attempts from 62 countries. The most active participants (> 50 accesses) come from a total of 27 countries. Swiss Post recorded the highest level of activity in the following countries:

Country	Number of IP addresses	Share
USA	28	19.2%
Switzerland	17	11.6%
France	17	11.6%
Germany	12	8,2%
United Kingdom	10	6.8%
India	7	4.8%
Tunisia	6	4.1%
Ireland	3	2.1%
Italy	3	2.1%
Other	43	29.5%
Total	**146**	**100.0%**

4.4. Attacks

4.4.1. Number of accesses

Of the 6,923 IP addresses that recorded activity in the public intrusion test, a total of 296,172 accesses originated from the pit.evoting.ch domain. 28,977 of these originated from the e-voting server, of which 9,665 are classified as attacks.

4.4.2.Status codes and number of attacks

For the accesses, the statistics with the HTTP status codes are as follows:

Code	Code Message	Number (on pit.evoting.ch)	Number (on pit.evot- ing.ch/vote)	Percentage (on pit.evot- ing.ch/vote)	Attack
200	OK	34,123	13,183	38.63%	-
302	Found	229	13	5.68%	-
304	Not Modified	7,776	6,053	77.84%	-
400	Bad Request	2,160	911	42.18%	Yes
401	Unauthorized	488	488	100.00%	Yes
403	Forbidden	231,038	8,182	3.54%	Yes
404	Not Found	19,905	11	0.06%	-
408	Request Timeout	103	20	19.42%	-
500	Internal Server Error	53	51	96.23%	Yes
405 406 413 415 417 429	Method Not Allowed Not Acceptable Content Too Large Unsupported Media Type Expectation Failed Too Many Requests	264	32	12.12%	-
502	Bad Gateway	33	33	100.00%	Yes
	Total	**296,172**	**28,977**	**49.57%**	-

General attacks on the e-voting infrastructure are listed in column 3. More targeted accesses on the e-voting server can be found in column 4. The error messages 400, 401, 403, 500 and 502 are added together to calculate the number of attacks.

As part of the intrusion test, many manipulated requests are sent to the server by the ethical hackers. These requests are answered by the server with an HTTP 400, 401, 403 or 500. The 33 requests with status code 502 "Bad Gateway" are attributable to the finding #YWH-PGM2323–210. The description and correction of the finding are described in section 4.1.

4.4.3. Vote casting

The ethical hackers were able to simulate the vote casting process 1:1 on the voting portal using sample voting cards.

A total of 385 sample voting cards were downloaded for this purpose.

The analysis of participants' accesses for each voting process step can be summarized as follows:

Process steps	Number of accesses
Login attempts	1,092
Successful logins	461
Failed logins	631
Vote submission successes	189
Vote submission fails	375
Successfully confirmed votes	157
Failed vote confirmations	211

In a real contest, there are usually only a few or no failed process steps. Here, the behaviour of eligible voters differs from that of ethical hackers..

4.4.4. OWASP ModSecurity Core Rule Set

Access to the e-voting system is protected by the web application firewall (WAF) OWASP ModSecurity Core Rule Set 3 (CRS). The CRS is configured to paranoia level 4, the highest level of protection available in the rule set. Swiss Post has been fine-tuning the CRS installation and the rule set for several years.

A total of 8,194 accesses were blocked due to alerts triggered by the CRS. Some of the alerts were ignored because they were below a specified value limit (anomaly threshold).

As a sponsor, Swiss Post supports the OWASP Core Rule Set cybersecurity framework. OWASP CRS, in combination with Apache ModSecurity, is one of the most effective IT security solutions available today. OWASP CRS is an open-source solution. By sponsoring the foundation, Swiss Post is supporting a security system that helps to strengthen cyber-security worldwide.

4.4.5. ModSecurity Allow List

To ensure that the CRS rule set does not generally block all access, certain values and parameters must be added to a list (whitelist). The list determines which requests are allowed.

The allow list is a second, complementary set of rules used in conjunction with CRS. Similar to a network firewall, this set of rules prohibits all access, and only a clearly defined list of permitted accesses can reach the server.

- An end user's access to the e-voting system is protected by a custom allow list that covers API endpoints (URIs), parameters and certain other access characteristics.
- It is technically possible that one access triggers one or more CRS and allow list rules before it is finally blocked or redirected to an encrypted port of the service. The numbers presented in the previous section are therefore not identical to the numbers presented here.
- A total of 185,733 accesses were blocked due to allow list breaches.

4.4.6. ModSecurity JavaScript Hash Check

Another protective measure is the hash check. A unique hash can be calculated for each file on a computer. As soon as a change is made to the file, the number changes. The hash check compares the check number of the file sent back to the voting client with the previously calculated check number entered in the ModSecurity configuration of the web application firewall to detect manipulations on the e-voting server. This security check aims to protect the security of the vote against internal attackers.

There were no indications of a potential internal attack.

Important: the Swiss Post e-voting system also enables voters, i.e., eligible voters in a real voting process, to check that the correct HTML and JavaScript files have been sent.[2] There were no messages that this check failed.

4.4.7. Additional security measures

The e-voting system has additional security measures that further minimize the risk of an external attacker reaching the e-voting server. These measures were not activated for the public intrusion test.

An example of another protective measure is the Fail2ban configuration, which blocks an IP address for a defined period of time after a certain number of incorrect access attempts. This configuration does not prevent attacks as a rule, but it makes penetration more difficult.

If the same configuration had been used in a live cantonal contest, 39% of the network traffic to the e-voting server registered during the public intrusion test would have been blocked by the active control/limitation of data traffic. To keep the access barrier for the experts low, Swiss Post has put this filtering system into simulation mode or deactivated it.

---

[2] https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/Security-advices/de/readme.md#hashwerte-%C3%BCberpr%C3%BCfen-erweiterte-pr%C3%BCfung

4.4.8. mod_qos

The mod_qos module is used to prevent DoS attacks. The aim is to slow down aggressive scanning activities, as these could pose a threat to the availability of the e-voting system. There is a zero tolerance policy in place with regard to scanning in the live e-voting environment and all detected scanning activities would be stopped immediately.

The following list shows the number of blocked access attempts per date from the public intrusion test:

Date	Number
2024-06-12	0
2024-06-13	0
2024-06-14	3
2024-06-15	17
2024-06-16	5
2024-06-17	55
2024-06-18	0
2024-06-19	3
2024-06-20	6
2024-06-21	0
2024-06-22	0
2024-06-23	0
2024-06-24	0
2024-06-25	0
2024-06-26	0
2024-06-27	3
2024-06-28	1
2024-06-29	1
2024-06-30	1
2024-07-01	7
2024-07-02	9
2024-07-03	1

5. Summary

Below is a summary of the key results from the public intrusion test of the Swiss Post e-voting system with complete verifiability from 17 June 2024 to 3 July 2024:

- **Participants:** Around 6,923 IP addresses took part in the public intrusion test. In total, Swiss Post recorded 146 IP addresses with more than 50 accesses to the e-voting server from the same IP address. 19.2 percent of these "most active participants" come from the United States of America, followed by Switzerland and France with 11.6% each. Compared to 2022 and 2023, more IP addresses took part, but the number of "most active participants" was lower.

- **Communication measures:** Swiss Post actively communicated information about the public intrusion test via various channels. It sent information in the run-up to, at the start of and during the test phase (via the bug bounty platform, e-government blog, mailings to the specialist community and institutional stakeholders, posts on the X and LinkedIn accounts for Swiss Post and the partner for the bug bounty programme).

- **Attacks:** With 6,923 different IP addresses, pit.evoting.ch was accessed over 296,000 times during the public intrusion test using the HTTP/HTTPS protocols, with around 9,500 of the accesses classified as attacks.

- **Findings:** None of the participants managed to penetrate the system. Swiss Post received four findings, of which it confirmed one. The finding did not concern any security-related aspects. It shows an improvement in the communication between the servers, making simultaneous requests impossible. Swiss Post has implemented the improvement in the voting server. The severity classification is "low". The person who reported the finding will receive a reward of 1,500 francs plus an additional bonus of 3,000 francs. Swiss Post has already resolved the finding.

The public intrusion test did not identify any security vulnerabilities despite the broad participation of ethical hackers, and at no time did it push operational systems to the limits of their capabilities. The IT security analyses show that Swiss Post's security standards were able to ward off all attempted attacks.