

E-voting system: Final report on public intrusion test

08.08.-02.09.2022

Contents

1. Management summary	2
2. Introduction	3
3. Preparatory work	4
3.1. Code of conduct	4
3.2. Organization	4
3.3. Scope of testing	4
3.4. Preparation of an electronic ballot	4
3.5. Communication	4
3.6. Conditions of participation	5
4. Results	6
4.1. Findings	6
4.2. Participants	7
4.2.1. pit.evoting.ch	7
4.2.2. pit-admin.evoting.ch	7
4.2.3. IP addresses by country	7
4.3. Attacks	8
4.3.1. Number of accesses	8
4.3.2. Status codes and number of attacks	8
4.3.3. Vote casting	8
4.3.4. OWASP ModSecurity Core Rule Set	8
4.3.5. ModSecurity allow list	8
4.3.6. ModSecurity JavaScript HashCheck	9
4.3.7. Additional security measures	9
4.3.8. mod_qos	9
5. Conclusion	10

Change record

This page shows the change status of this document. A new version is issued after each change.

Version	Creator	Date
1.0	Swiss Post e-voting team	27.09.2022

1. Management summary

Swiss Post conducted a public intrusion test (PIT) on its electronic voting (e-voting) system. 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 trials¹.

For four weeks, from 8 August to 2 September 2022, ethical hackers attacked the Swiss Post e-voting infrastructure. Interested parties were able to test the infrastructure that will be used as part of the system for elections and votes in future. The ethical hackers were able to try out and target the vote casting process on the voting portal using sample voting cards, just as voters will do in the future.

The test attracted strong interest on the professional scene: there were more than 60,000 attacks on the system from 3,400 IP addresses. More than 50 accesses were attempted from each of 178 of the recorded IP addresses. These are referred to as the “most active participants” in this report.

None of the hackers managed to penetrate the system. Swiss Post received two findings and confirmed one with low severity after testing.

The confirmed finding does not affect any security-related aspects, but it does help to streamline processes on the voting portal. Swiss Post will implement this improvement in the form of best practice and has paid the ethical hacker a reward of CHF 500.

The second finding concerned the application for downloading a sample voting card which Swiss Post provided for the public intrusion test, so that hackers could try out the electronic voting process. In a real contest, voters do not download the voting cards themselves, but instead receive them by post. This finding was therefore outside the defined scope of the PIT and was accordingly not confirmed.

The successful completion of the public intrusion test in accordance with the Confederation’s directives for the e-voting trial is therefore a further step towards the provision of the system.

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. It 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.

As part of a community programme, Swiss Post has disclosed all of the main components and documents of its future 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 and simulate attacks. During the public intrusion test, Swiss Post expanded the options available for testing: for four weeks, from 8 August to 2 September 2022, ethical hackers were able to attack the Swiss Post e-voting infrastructure. Interested parties had a direct experience with the infrastructure that will be used as part of the system for elections and votes. For the first time ever, ethical hackers were also able to try out the vote casting process on the future e-voting system using sample voting cards and target the system.

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 should also be made possible in a permanent programme or as a recurring test with a limited duration.

Swiss Post is implementing these requirements and opening up the following testing options for its system to experts:

Permanent, no time limit	Regular implementation, always for a limited time
<ul style="list-style-type: none">– Static tests: Search for errors and vulnerabilities in the published documents and in the source code for the e-voting software. All published elements are always part of this testing.– Dynamic tests: researchers 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.	Public intrusion test: attacks on the system and attempts to infiltrate the electronic infrastructure

Swiss Post launches its bug bounty programmes in stages, i.e. it starts with a group of experts and expands the group continuously until it opens a programme, invites all interested parties to participate and informs the public. This phased approach is common in the industry for collaboration with ethical hackers.

For the e-voting system, Swiss Post launched a bug bounty programme in 2021 with a limited group of hackers (“private programme”). Participants were able to test all key system components and documentation, and could also attack the infrastructure. Seven confirmed findings were received from this “private intrusion test” by August 2021.

In the period from 8 August to 2 September 2022, Swiss Post conducted the public intrusion test and allowed ethical hackers to test the infrastructure by attacking it. A four-week period is the usual duration of a contest in most cantons (the period from sending the voting documents to counting the votes). Swiss Post would like to carry out the tests on the infrastructure intended for use in the cantons. To ensure that no contests are disrupted, this is only possible if a limited test window is available.

This report summarizes the findings of the public intrusion test.

3. Preparatory work

3.1. Code of conduct

Swiss Post 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. The code of conduct for the community programme is available online (<https://evoting-community.post.ch/en/code-of-conduct>).

In addition, rules apply for participation in the public bug bounty programme 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 with the independent company YesWeHack. The YesWeHack platform is the access point to the bug bounty programme and the reporting office for findings. After initial triage of the reports coming in from the team at YesWeHack, a specialist Swiss Post team analysed the findings.

3.3. Scope of testing

Part of the public intrusion test was an exact copy of the e-voting system's productive environment, referred to in this report as "infrastructure". For this purpose, Swiss Post provided the same system infrastructure that is planned for use in the cantons in elections and votes.

3.4. Preparation of an electronic ballot

In the preparation of 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 the integrated provider (Swiss Post) in the preparation of the electronic ballot is a security measure and a legal requirement of the Confederation.

For the test setting, i.e. for the public intrusion test, Swiss Post assumed responsibility for all preparatory work, i.e. the provision of the ballot boxes, voting cards and e-voting infrastructure.

The electronic ballot for the public intrusion test was defined as follows:

- A fictional federal vote, not an election
- The two voting options were formulated in a neutral way. The answers to these were YES, NO or EMPTY.
- 5,000 sample voting cards were provided to allow the hackers to accurately try out the electronic vote casting process.

The sample voting cards were made available without prior registration via a dedicated 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. It publishes the confirmed findings on the specialist platform GitLab.

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](#)

Swiss Post classifies findings of the community programme into four levels of severity (low, medium, high, critical). Swiss Post also describes all findings with a high or critical severity level for a wider audience on the [e-voting blog](#).

Swiss Post drew attention to the public intrusion test through various channels at its launch and as it progressed:

- Distribution of fliers on the occasion of Le Hack in Paris (25/26 June 2022)
- 08.08.2022: Press release, e-voting blog post, newsmail to the e-voting community
- 18.08.2022: Media blog with an interview with an ethical hacker
- Various activities on social media, including tweets on the Swiss Post Twitter channels and the platform operator YesWeHack

3.6. Conditions of participation

No registration was required to participate in the PIT. Registration was required only if an ethical hacker wished to submit a finding via the YesWeHack bug bounty platform in order to receive a reward. All contact details remained with YesWeHack and were 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

4.1. Findings

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 scale². This scale is based on a common standard for the categorization of security findings.

Swiss Post received two reports of findings in total, and after analysing the findings, was able to confirm one finding with a "low" severity. The second finding was not part of the scope of the intrusion test.

The confirmed finding shows that processes on the voting portal can be streamlined. The finding is described below.

Title	Inactive voting cards can be used to disclose the voting options
Classification	Low
Number	#YWH-PGM2323-92
Date of receipt	02.09.2022
Reported by	Dharmaraj PS
Description	<p>If a person with malicious intent obtains an invalid voting card, e.g. from a person who has already cast a vote, they can manipulate the voting portal into displaying information that is not required for the process step but is not sensitive.</p> <p>In the back end of the voting portal, not only is a message sent indicating that the voting card has been deactivated, but the voting options that can be found on the ballot are also transmitted.</p> <p>An online system should only pass on the necessary information, not more. The response from the back end should not reproduce the content of the voting card.</p>
Status	<p>All the pre-printed ballot content is public, so it is not sensitive information and there is no risk to the security or confidentiality of electronic voting.</p> <p>This finding was classified as best practice.</p> <p>Swiss Post has confirmed the finding and will carry out the improvement in the system.</p>
Reward	The reporter has received a reward of CHF 500.

The second finding reported concerned the application for downloading a sample voting card which Swiss Post provided for the public intrusion test, so that hackers could try out the electronic voting process. In a real contest, voters do not download the voting cards themselves, but instead receive them by post. This finding was therefore outside the defined scope of the PIT.

Further information on the findings received during the public intrusion test on the other test areas (scopes) in the e-voting community programme can be found at:

– [Results from the bug bounty programme, update 28 September 2022](#)

² [Common Vulnerability Scoring System Version 3.1 Calculator \(first.org\)](#)

4.2. Participants

For the public intrusion test, Swiss Post prepared a test ballot using the same infrastructure intended for use and set it up as a real contest.

All IP addresses assigned to the domains 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) and the cantonal administration portal (pit-admin.evoting.ch), each with its own IP address.

4.2.1.pit.evoting.ch

- During the PIT, the pit.evoting.ch server was accessed from around 3,400 different IP addresses via the HTTP/HTTPS protocols.
- 61 IP addresses attempted to cast votes via pit.evoting.ch.
- 58 IP addresses successfully cast at least one vote.
- Of a total of 178 IP addresses, more than 50 accesses to the e-voting server were granted. These are referred to as the “most active participants”.

4.2.2.pit-admin.evoting.ch

During the PIT, 389 different IP addresses provided access to the administration portal via HTTP/HTTPS.

The administration portal only permits access if a valid client certificate is used for authentication. As a result, not a single successful access to the administration portal was possible. Instead, the access was detected by the system and blocked as unauthorized access. The rest of the report focuses on the e-voting server (voting portal).

4.2.3.IP addresses by country

Among the most active IP addresses (> 50 accesses), the following countries are most represented:

Country	Number of IP addresses	Percentage
Switzerland	48	26.97%
USA	34	19.10%
Germany	17	9.55%
Netherlands	13	7.30%
France	11	6.18%
Tunisia	11	6.18%
Russia	6	3.37%
India	5	2.81%
Great Britain	4	2.25%
China	3	1.69%
Singapore	3	1.69%
Australia	2	1.12%
Belgium	2	1.12%
Czech Republic	2	1.12%
Spain	2	1.12%
Ukraine	2	1.12%
Other	13	7.31%
Total	178	100.00%

4.3. Attacks

4.3.1. Number of accesses

- Of the 3,400 IP addresses that recorded total activity during the PIT, 3,781,240 accesses originated.
- Of the 178 IP addresses that recorded the most activity in the PIT, a total of 150,125 accessed the e-voting server.
- This means that on average there were 843 accesses with a median value of 112 accesses per IP address.

4.3.2. Status codes and number of attacks

For the 150,125 accesses, the statistics with the http status codes are as follows:

Code	Code Message	Number	Percentage	Attack
200	OK	73,479	48.95%	
301	Moved Permanently	7,821	5.21%	
304	Not Modified	482	0.32%	
400	Bad Request	1,221	0.81%	1,221
403	Forbidden	61,796	41.16%	61,796
404	Not Found	4,435	2.95%	
408	Request Timeout	819	0.55%	
500	Internal Server Error	72	0.05%	72
Total		150,125	100.00%	63,089

The absence of status code 502 “Bad Gateway” indicates that availability of the back-end systems was good.

The 72 accesses that resulted in status code 500 “Internal Server Error” are due to incorrectly coded accesses to the server. In the public intrusion test, no findings were reported that would have referred to status code 500.

4.3.3. Vote casting

The ethical hackers were also able to simulate the voting process on the voting portal with sample voting cards in the same way as a future voter.

The analysis of participants’ access rights per voting process step can be summarized as follows:

Process steps	Number of accesses	
Login attempts	1,706	from 98 different IP addresses
Successful logins	332	from 85 different IP addresses
Failed logins	1,374	from 44 different IP addresses
Successes with authentication tokens	228	from 79 different IP addresses
Failed attempts with authentication tokens	14	from 4 different IP addresses
Vote submission successes	82	from 59 different IP addresses
Vote submission fails	7	from 3 different IP addresses
Successfully confirmed votes	79	from 58 different IP addresses
Failed vote confirmations	12	from 3 different IP addresses

In a real contest, the number of failed accesses is significantly lower than in the intrusion test performed.

4.3.4. 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. As a result, there were very few false positives.

A total of 53,537 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).

4.3.5. ModSecurity allow list

To ensure that the CRS policy does not generally block all access, certain values and parameters must be added to a list

(whitelist). The list generally 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 access rights can access 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 65,666 accesses were blocked due to allow list breaches.

4.3.6. ModSecurity JavaScript Hash Check

Another protective measure is the HashCheck. 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 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.

- The JavaScript files returned to the vote clients are tested for consistency on the way to the client. This security check aims to protect the security of the vote from internal attackers.
- 4,323 accesses passed the test successfully.
- Note that no finding has been reported regarding this possible abnormal behaviour.

4.3.7. 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 certain period of time after a certain number of incorrect accesses have been received. This configuration does not prevent attacks in principle, but its delay measures do make penetration more difficult.

If the same configuration had been used in a productive 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 researchers low, our filtering system was put into simulation mode or deactivated.

4.3.8. 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 productive 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 PIT:

Date	Number
08.08.2022	1,545
09.08.2022	32
11.08.2022	32
15.08.2022	59
17.08.2022	32
19.08.2022	32
20.08.2022	64
21.08.2022	66
22.08.2022	60
25.08.2022	21
26.08.2022	32
27.08.2022	32
29.08.2022	81
01.09.2022	96

5. Conclusion

Below is a summary of the key results from the public intrusion test of the Swiss Post e-voting system from 08.08-02.09.2022:

- **Participants:** 3,400 people (IP addresses) took part in the public intrusion test. Most requests from IP addresses originate geographically in the USA and China. In total, Swiss Post has recorded 178 IP addresses with more than 50 accesses to the e-voting server. A good quarter of these “most active participants” come from Switzerland, around 20 percent from the USA and 10 percent from Germany.
- **Findings:** Swiss Post received two findings, one of which it has confirmed. The latter is best practice (low severity) and concerns an improvement to streamline the processes on the voting portal. Swiss Post is implementing the improvement and has paid the reporter a reward of CHF 500.
The second finding concerned the application for downloading a sample voting card which Swiss Post provided for the public intrusion test, so that hackers could try out the electronic voting process. In a real contest, voters do not download the voting cards themselves, but instead receive them by post. This finding was therefore outside the defined scope of the PIT.
- **Attacks:** with around 3,400 different IP addresses, the e-voting server was accessed over 3.7 million times during the public intrusion test using the HTTP/HTTPS protocols. The cantonal administration portal was accessed via HTTP/HTTPS from 389 different IP addresses. The 178 most active participants made a total of 150,125 access to the e-voting servers, of which over 60,000 are classified as attacks.

The PIT 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 stave off any attempts at attack within the defined framework.