

Final report on the e-voting public intrusion test

8 July 2023 – 31 July 2023

Table of contents

1. Management summary	2
2. Introduction	3
3. Implementation of the PIT	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. Other findings that were not accepted	7
4.3. Participants	9
4.4. Attacks	10
5. Summary	14

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 trial operations¹.

From 8 to 31 July 2023, ethical hackers had the opportunity to conduct attacks on Swiss Post’s e-voting system infrastructure. Interested parties were able to test the infrastructure that is planned for use in the system for elections and votes. The ethical hackers 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 more than 53,000 attacks on the system from 2,650 IP addresses. More than 50 attempts at access were made from 273 of the IP addresses registered. These are referred to in this report as the “most active participants”.

None of the hackers managed to penetrate the system. Swiss Post received four findings and confirmed one with low severity after testing. The findings did not relate to any security-related aspects and demonstrated an improvement in the reverse proxy configuration in the e-voting web infrastructure. Swiss Post has already implemented this improvement. The hacker received a reward of 1,000 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.

For e-voting, the Swiss 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 implements these requirements 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 new 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

Through the public intrusion test, Swiss Post periodically offers another test option: ethical hackers can attack the system in the 1:1 infrastructure. They encounter the same infrastructure that Swiss Post provides when using the system for real elections and votes. After last year's intrusion test in autumn 2022, another public intrusion test took place in July 2023.

This report summarizes the findings of the 2023 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. The code of conduct for the community programme is 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 the reporting point for findings. After initial triage of the reports sent in by 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 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.

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

- A fictitious ballot with 5 lists, 23 candidates and 5 seats that can be filled fictitiously.
- Swiss Post provided 5,000 sample voting cards to allow the hackers to test the electronic vote casting process accurately.

The sample voting cards could be downloaded without prior registration from 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. 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](#)

Swiss Post classifies findings from 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-voting blog](#).

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

- 14.06.2023: Direct message (announcement) via the bug bounty platform to researchers known to Swiss Post

- 07.07.2023: Direct message via the bug bounty platform to well-known researchers as a reminder of the upcoming launch
- 12.07.2023: Article on the e-voting blog and news sent to a defined circle of interested media, information e-mail to the specialist community and institutional stakeholders, political newsletters, posts on the Twitter and LinkedIn accounts for both Swiss Post and the bug bounty programme partner
- 19.07.2023: Posts on the Twitter and LinkedIn accounts for both Swiss Post and the bug bounty programme partner regarding a bonus of €3,000 (in addition to the regular rewards) for the first three experts to report a confirmed finding
- 27.07.2023: Interview with the first expert to report a confirmed finding on the e-voting blog, posts about the interview and the remaining five days of the intrusion test on the Twitter and LinkedIn accounts for both Swiss Post and the bug bounty programme partner
- 16.08.2023: Article on the Swiss Post media blog about the results of the public intrusion test

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 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 analysing the findings, it was able to confirm a finding with a “low” severity. The other three findings were not confirmed and were closed as “informative”.

The confirmed finding demonstrated an improvement in the reverse proxy configuration in the e-voting infrastructure.

Title	Reverse-proxy Insufficiently Validates Input in a specific case when Redirecting Requests to Another Location
Classification	Low
Number	#YWH-PGM2323-187
Date of receipt	13.07.2023
Reported by	Vladyslav Zubkov (schwytz)
Description	<p>Each request to the e-voting system passes through a reverse proxy web server. This reverse proxy performs various validations and includes a web application firewall. The Infrastruktur Whitepaper explains the role of the reverse proxy. Occasionally, the reverse proxy performs HTTP redirecting. HTTP redirects are a standard way to inform a client, like a web browser, that the requested URL has been changed, and a different URL should be accessed instead. It's a mechanism employed by web servers to redirect a user's browser automatically to another location.</p> <p>If a request contains a specific non-standard HTTP request header, the reverse proxy redirects the client to a domain that is provided by the request's "Host" value. The reverse proxy should redirect the client only to a resource that has the same domain (for instance, pit.evoting.ch) and not to a different domain that might be controlled by an attacker. Currently, the reverse proxy does not correctly validate the “Host” value in the request header and accepts values such as pit.evoting.ch.another.com. It is possible – albeit only theoretically – to redirect a client to an incorrect website</p> <p>It is not possible in practice, however, due to the security measures that prevent an HTTP request from being intercepted. Nevertheless, the reverse proxy should correctly validate the “Host” header field and accept only expected domains entered in this field.</p>
Status	<p>The researcher points out that the vulnerability is very unlikely to be exploitable by an attacker to have a realistic attack scenario. This means it's easy to use as a self-own; however, it's impractical to exploit anyone else with it.</p> <p>This report is considered a best practice violation and does not demonstrate an attack vector or a vulnerability. Nevertheless, the reverse proxy's configuration will be corrected to prevent this behaviour. Swiss Post has confirmed the finding and corrected the configuration in the system.</p>
Reward	The reporting expert received a reward of CHF 1,000 and an additional bonus of CHF 3,000.

4.2. Other findings that were not accepted

Title	Encountering Invalid Authentications when Intercepting Requests
Number	#YWH-PGM2323-185
Date of receipt	08.07.2023
Reported by	No Breach
Description	The hunter intercepted requests and modified them in various ways. Even though the hunter used the correct start voting key and date of birth, the voting server replied with an HTTP 401 Unauthorized status to the intercepted requests. The hunter opened an issue to check whether this indicates a problem with the authentication protocol.
Status	<p>Closed as Informative.</p> <p>The authentication protocol, which is loosely based on the widely used TOTP (Time-based One-time Password) mechanism, checks the "freshness" of a request.</p> <p>If a person intercepts the request for more than 30 – 60 seconds, the authentication challenge is no longer "fresh" and the voting server correctly refuses the authentication challenge. Therefore, this behavior is by design.</p>
Reward	None

Title	Supposed bypass of vote confirmation
Number	#YWH-PGM2323-184
Date of receipt	08.07.2023
Reported by	Xiety
Description	The hunter conjectured that it is possible to bypass the vote confirmation by simply returning to the voting client the response of a successful confirmation (that could be obtained, for instance, from a different voting card) - even though the voter did not enter the correct confirmation code.
Status	<p>Closed as informative. This report demonstrates no discernible impact on security beyond the user's own client use. The mechanism identified is only possible when exercised on the user's own computer. It would not be possible for a third party to tamper with it, and thus there is no risk to the correct and secure casting of votes. A voting person cannot in any case - either alone or with the help of a third person - confirm a vote without entering their confirmation code.</p> <p>From the server, the attempt to cast a vote with an invalid confirmation code was not taken into account by the evoting system, as can be seen from the server response: " CONFIRMATION_KEY_INVALID". Therefore, the vote remains in the unconfirmed state and is not counted in the election, so no security impact was achieved.</p>
Reward	None

Title	Supposed possibility to cast multiple votes.
Number	#YWH-PGM2323-186
Date of receipt	08.07.2023
Reported by	Xiety
Description	The hunter conjectured that it is possible to cast multiple votes for a single voter. Potentially, a voter could download multiple voting cards and use them to vote multiple times for the same election. There are no restrictions (for instance based on the IP address) for downloading voting cards.
Status	Closed as Informative. The sample voting card provided on https://www.evoting.ch/vc/ is explicitly provided for testing purposes. During the PIT user can generate as many cards as they need. However, in an actual election, a single voting card will be sent by mail to each voter.
Reward	None

The findings are classified according to the [Common Vulnerability Scoring System Version 3.1 Calculator \(first.org\)](#).

4.3. Participants

For the public intrusion test, Swiss Post prepared a test ballot using the same infrastructure that is planned for live use and set it up to resemble a real ballot.

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 PIT, the pit.evoting.ch server was accessed from around 2,650 different IP addresses via the HTTP/HTTPS protocols.
- 42 IP addresses attempted to cast votes via pit.evoting.ch.
- 32 IP addresses successfully cast at least one vote.
- Of a total of 273 IP addresses, more than 50 accesses to the e-voting server were granted. These are referred to as the “most active participants”.

4.3.1. IP addresses by country

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

Country	Number of IP addresses	Percentage
Germany	59	21.61%
USA	55	20.15%
Switzerland	27	9.89%
France	20	7.33%
Canada	13	4.76%
India	12	4.40%
Czech Republic	7	2.56%
Lithuania	5	1.83%
Portugal	5	1.83%
Singapore	5	1.83%
Finland	4	1.47%
Tunisia	4	1.47%
Vietnam	4	1.47%
Belgium	3	1.10%
Romania	3	1.10%
Russia	3	1.10%
Turkey	3	1.10%
United Kingdom	3	1.10%
Others/unknown	38	13.92%
Total	273	100.00%

4.4. Attacks

4.4.1. Number of accesses

- From the 2,650 IP addresses that recorded total activity during the PIT, there were 471,141 accesses.
- On average there were 178 accesses, with a median of three accesses per IP address.
- Of the 273 IP addresses that recorded the most activity in the public intrusion test, a total of 446,661 accesses originated from the pit.evoting.ch domain. 89,708 of these originated from the e-voting server, of which over 53,000 are classified as attacks.

4.4.2. Status codes and number of attacks

For the 446,661 accesses, the statistics with the HTTP status codes are as follows:

Code	Code message	Number (on pit.evoting.ch)	Number (on pit.evoting.ch/vote)	Percentage (on pit.evoting.ch/vote)	Attack
200	OK	26,511	10,587	11.80%	-
302	Found	33,884	21,181	23.61%	-
304	Not Modified	7,114	4,204	4.69%	-
400	Bad Request	12,961	1,532	1.71%	Yes
401	Unauthorized	5,023	0	0%	Yes
403	Forbidden	359,745	52,052	58.02%	Yes
404	Not Found	399	122	0.14%	-
408	Request Timeout	233	28	0.03%	-
500	Internal Server Error	694	0	0%	Yes
405 406 413 415 417 429	Method Not Allowed Not Acceptable Content Too Large Unsupported Media Type Expectation Failed Too Many Requests	97	2	0%	-
Total		446,661	89,708	100%	-

General attacks on the e-voting infrastructure are listed in column 3. More targeted attacks on the e-voting server can be found in column 4.

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

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.

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

Process steps	Number of accesses	
Login attempts	12,304	from 74 different IP addresses
Successful logins	239	from 49 different IP addresses
Failed logins	12,065	from 25 different IP addresses
Vote submission successes	82	from 38 different IP addresses
Vote submission fails	19,645	from 12 different IP addresses
Successfully confirmed votes	59	from 32 different IP addresses
Failed vote confirmations	16,112	from 10 different IP addresses

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

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 13,390 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).

4.4.5. 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 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 177,262 accesses were blocked due to allow list breaches.

4.4.6.ModSecurity JavaScript HashCheck

Another protective measure is the hash check. A unique check number (hash) can be calculated for each file on a computer. As soon as a change is made to the file, this number changes. The hash check compares the check number of the file sent back to the voting client with the check number previously calculated and entered in the ModSecurity configuration of the Web Application Firewall in order to detect manipulations on the e-voting server. This security check is to ensure the protection of the voting against internal attackers.

Statistics:

- 5,039 accesses passed through this check successfully.
- For 50 accesses, this check failed and the file was not sent to the voting client. The analysis showed that these were false positives where the voting client prematurely aborted the request. We are looking into how to avoid these false positives in the future.
- Note that no finding has been reported regarding these possible manipulations.

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 certain period of time after a certain number of incorrect accesses have been received. This configuration does not prevent attacks in principle, 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.

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 PIT:

Date	Number
08.07.2023	24
09.07.2023	0
10.07.2023	0
11.07.2023	0
12.07.2023	0
13.07.2023	0
14.07.2023	33
15.07.2023	0
16.07.2023	0
17.07.2023	3
18.07.2023	66
19.07.2023	0
20.07.2023	0
21.07.2023	0
22.07.2023	0
23.07.2023	33
24.07.2023	0
25.07.2023	0
26.07.2023	0
27.07.2023	33
28.07.2023	33
29.07.2023	33
30.07.2023	0
31.07.2023	0

5. Summary

Below is a summary of the key results from the public intrusion test of the Swiss Post e-voting system from 8 July 2023 to 31 July 2023:

- **Participants:** Around 2,650 IP addresses took part in the public intrusion test. In total, Swiss Post has recorded 273 IP addresses with more than 50 accesses from the same IP address to the e-voting server. Over 20% of these “most active participants” come from Germany, around 20% from the USA and 10% from Switzerland. Compared to last year (2022), around 1,000 fewer IP addresses took part, but the number of “most active participants” was a third higher.
- **Communication measures:** Swiss Post has actively communicated information about the public intrusion test via various channels. The company shared information before, at the start of and during the test. Bug bounty platform, e-voting blog, mailings to the specialist community and institutional stakeholders, newsletters, posts on the Twitter and LinkedIn accounts for both Swiss Post and the bug bounty programme partner, communicated before and during the PIT. On 27 July 2023, an interview with the first expert to report a confirmed finding was conducted on the e-voting blog. Posts were also made about the interview and about the remaining five days of the intrusion test on the Twitter and LinkedIn accounts for both Swiss Post and the bug bounty programme partner.
- **Attacks:** With around 2,650 different IP addresses, the e-voting server was accessed over 472,000 times during the public intrusion test using the HTTP/HTTPS protocols, with over 53,000 of the accesses classified as attacks.
- **Findings:** None of the hackers managed to penetrate the system. Swiss Post received four findings, of which it confirmed one. The finding concerns an improvement to the proxy configuration, which is considered a best practice. The severity classification is “low”. Swiss Post paid the reporting expert a reward of CHF 4,000 and is implementing the improvement.

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.