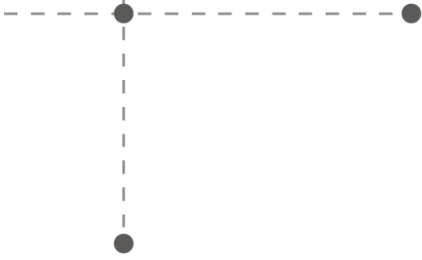




**Cyberdefense**



**Federal Chancellery**

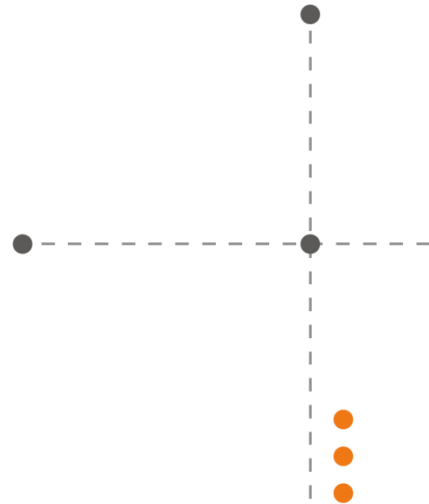
# E-voting Web Application

## 1.4.4.4

**Security Audit Report**

**December 2024**

<b>Reference</b>	P022453
<b>Last modified</b>	2025-01-07
<b>Classification</b>	Unrestricted



## Client contact information

---

Federal Chancellery ChF

## Contact

---

Orange Cyberdefense Switzerland SA  
Rue du Sablon 4  
1110 Morges  
Switzerland

## Versions

Date	Version	Author	Description
2024-12-05	0.1		Initial Document
2024-12-06	0.2		Added summaries
2024-12-12	1.0		Review
2024-01-06	1.1		Review for publication

## Table of contents

<b>Executive summary</b>	<b>4</b>
Results summary	4
High level impressions	4
Security dashboard	5
Global risk level	5
Status by attacker profile	5
<b>Technical summary</b>	<b>6</b>
Scope	6
Restrictions	6
Results	6
Informational findings	7
<b>Detailed results</b>	<b>8</b>
Vulnerabilities and exploitation	8
Informational findings	8
P022453-01 Outdated system or software	8
<b>Complements</b>	<b>9</b>
Legend	9
Orange Cyberdefense Switzerland Score	9
CVSS Score	9
Risk calculation	10
Context	10

## Executive summary

### Results summary

The Federal Chancellery contracted Orange Cyberdefense SA to perform a comprehensive security assessment of the e-voting Web application developed by the Swiss Post. This assessment followed a white-box approach, where the source code and a number of voting cards were provided by Swiss Post. This approach allowed the engineers to thoroughly analyse the application's codebase and functionality to uncover potential security vulnerabilities.

The primary objective of this assessment was to simulate realistic cyberattacks that adversaries might employ to compromise the confidentiality or integrity of e-voting campaigns.

During the evaluation, the team identified one single finding that was classified as informational, because no way of exploiting the issue was discovered. Importantly, no security risks or exploitable vulnerabilities were observed. The informational finding pertained to outdated dependencies in the application's codebase. While these dependencies are no longer current, none of the related updates introduced fixes for vulnerabilities that might impact the application.

From a voter's perspective, the attack surface is very limited, and a reverse proxy additionally filters out invalid inputs. Cryptographic operations are also used to further restrict malicious operations.

Overall, the risk level of the application is therefore considered as very low.

### High level impressions

#### Strengths

- + WAF configuration
- + Parameter filtering and validation
- + Data confidentiality
- + Limited attack surface

#### Weaknesses

- Outdated component

## Security dashboard

<b>Type</b>	White-box	<b>Schedule</b>	2024-12-02 – 2024-12-06
<b>Scope</b>	Web application	<b>Effort</b>	10 days

### Global risk level

Attacker profiles	Risk level
Without voting card	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
With voting card	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

### Status by attacker profile

Objectives	Without voting card	With voting card
Gain access to the internal network	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Execute arbitrary commands on a server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Vote confidentiality and integrity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Application infrastructure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> NOT COMPROMISED	<input type="checkbox"/> <input checked="" type="checkbox"/> PARTIALLY COMPROMISED	<input type="checkbox"/> <input checked="" type="checkbox"/> COMPROMISED

## Technical summary

### Scope

The scope of the audit includes the e-voting web application (release 1.4.4.4), which was reachable during the audit at the following address:

<https://it.evoting.ch/vote/#/legal-terms/3E46F60830DE9328504A13CB13985487>

One thousand voting cards were also provided to the auditors for the related event. The penetration test was performed as a white-box audit, the source code of the application was also available on GitLab:

<https://gitlab.com/swisspost-evoting>

### Restrictions

No social engineering or denial of service attacks were performed during this audit.

### Results

As this assessment was performed in a white-box context, the engineers started the audit by using automated code analysis tools to examine the source code, before reviewing it manually. Nothing relevant was found in the allotted time, except the use of outdated components in the 1.4.4.4 e-voting Maven configuration files release (`pom.xml`). However, the security issues they entail are not exploitable within the e-voting application context, as the prerequisites are not met. Therefore, this finding is only considered as informational.

The second day of the audit, a voting event was set up for testing and the corresponding URL was shared with the auditors, along with valid voting cards. The use of automated tools did not allow to find any vulnerabilities. Therefore, a more thorough manual investigation was carried out to gain a deeper understanding of the application's functionality. Once the web application was mapped out, the engineers proceeded to test each component individually, from the authentication process to the vote submission. Particular attention was given to the authentication process, as it is an integral part to nearly every request. The auditors employed various methods, including injection techniques, race conditions, and other tactics, in an attempt to compromise the vote's integrity, but all efforts proved unsuccessful.

The auditors then attempted to deploy the infrastructure locally, but several issues during the building and deployment processes were encountered. This investigation did not lead to any additional findings.

In conclusion, no security issues were identified during this audit, the risk level is therefore considered as low.

## Informational findings

ID	Finding
P022453-01	Outdated system or software

## Detailed results

### Vulnerabilities and exploitation

#### Informational findings

INFO	P022453-01 Outdated system or software	
	PREREQUISITES	COMPROMISED ASSETS
	-	-

#### Vulnerable components

- <https://gitlab.com/swisspost-evoting/e-voting/e-voting/-/blob/933f284f50d0f5dc5a7c61b3bb35eec48ab2ef/pom.xml>

#### Description

An outdated system, or a system using outdated software is more likely to be prone to attacks than a system with all updates and patches installed. A regular update is mandatory in order to correct issues that could enable an attacker to compromise the normal behaviour of the application.

#### Exploitation

By assessing the `pom.xml` files, the following versions were outdated at the time the report was written (as of 06.12.2024):

- maven-dependency-check used version 10.0.4 - current version 11.1.1
- maven-javadoc-plugin used version 3.10.1 - current version 3.11.1
- versions-maven-plugin used version 2.17.1 - current version 2.18.0
- spring-boot-maven-plugin used version 3.3.4 - current version 3.3.6 or 3.4.0

The spring-boot-maven-plugin update addresses the vulnerability identified in [CVE-2024-38820](#).

None of the issues were exploitable during this assessment.

#### Possible solutions

##### Apply security updates:

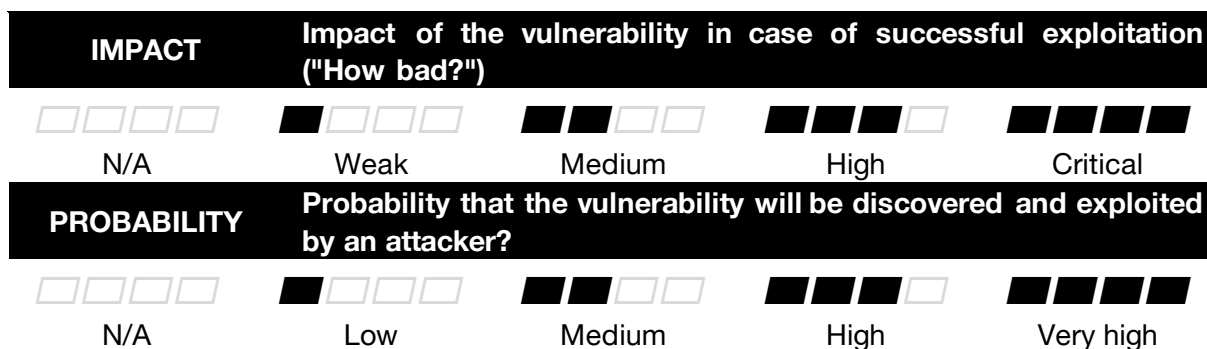
Regularly reviewing project dependencies to identify any vulnerabilities or outdated versions. That can be done manually or by implementing automated tools for monitoring and managing them.

## Complements

### Legend

#### Orange Cyberdefense Switzerland Score

For each vulnerability discovered and detailed in this report, Orange Cyberdefense Switzerland provides a threat assessment based on two indicators, an **Impact** and a **Probability** of exploitation.



However, it is important to keep in mind that this assessment is solely based on the information available to the engineers at the time of the audit. The engineers are not necessarily aware of all the details regarding the vulnerable applications or systems. Consequently, these ratings should always be reconsidered based on the context of the information system as a whole.

#### CVSS Score

In addition to its own scoring system, Orange Cyberdefense Switzerland also provides an evaluation based on the **Common Vulnerability Scoring System (CVSS)**, for each vulnerability.

As a reminder, CVSS is a vulnerability scoring system designed to provide an open and standardised method for rating IT vulnerabilities. CVSS helps organisations prioritise and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of a vulnerability. More information about the CVSS scoring system can be found here: <https://www.first.org/cvss/user-guide>

## Risk calculation

Each risk presented in this report is calculated as the product of an **impact** and a **probability** of exploitation, as defined in the matrix below.

		Overall Risk Severity			
		High	High	Critical	Critical
Impact	CRITICAL	High	High	Critical	Critical
	HIGH	Moderate	Moderate	High	Critical
	MODERATE	Low	Moderate	Moderate	High
	LOW	Low	Low	Moderate	High
		LOW	MODERATE	HIGH	CRITICAL
		Probability			

Orange Cyberdefense Switzerland provides an estimation of the effort required to fix each vulnerability and thus mitigate their associated risk. It should be noted that this assessment is based on Orange Cyberdefense Switzerland's experience, and as such might not fully reflect the context of the company or organisation.

## Context

The context of each vulnerability is defined by its prerequisites and a list of compromised assets. The prerequisites represent the conditions that are required for the exploitation of a given vulnerability (*e.g.*: social engineering). Compromised assets represent the theoretical or tangible result of its exploitation (*e.g.*: a user account).