# Vulnerability Report – Swiss Post E-Voting System – Browser V1.0

28.06.2023, Andreas Kuster, *[email, redacted]*

## Abstract

In this report, we will showcase using a proof of concept of a malicious browser plugin injected into the voting client's browser, how to extract the votes (voter secrecy) and manipulate user votes without the user and the auditor being able to detect the fraud (individual verifiability).

The malicious browser plugin can be seen as an undetectable virus as described in [Explanatory Report, Sec 4.2.1].

*[Explanatory Report, Sec 4.2.1]: With individual verifiability, voters can detect any deliberate or inadvertent misuse of their voting rights. This should be possible even if the user device or the transmission path are not trustworthy. It must be assumed a priori that the user device or transmission path contains undetectable viruses or has been otherwise tampered with.*

*[OEV, Art. 5, Sec 2] The requirements for individual verifiability are as follows:*

*a. The person voting is given the opportunity to ascertain whether the vote as entered on the user device has been manipulated or intercepted on the user device or during transmission; to this end, the person voting receives proof that the trustworthy part of the system (Art. 8) has registered the vote as it was entered by the person voting on the user device as being in conformity with the system; proof of correct registration is provided for each partial vote.*

*b. A voter who has not cast his or her vote electronically can request proof after the electronic voting system is closed and within the statutory appeal deadlines that the trustworthy part of the system has not registered any vote cast using the client-side authentication credential of the voter.*

In this report, we first showcase the working principles of the attack in theory, followed by a proof-of-concept implementation and demonstration. Finally, we propose remedies to mitigate and reduce the risk imposed by this attack.

## Proof of Concept Attack

In order to understand the functionality of the malicious browser plugin that is installed on the voting client, we first look at the modified voting protocol played by the three parties.

**Protocol**

| User/Voter | Malicious Browser Extension | Swiss Post Voting Server* |
|---|---|---|
| Visit voting website (here: localhost:7000, otherwise for example sg.evoting.ch) | | |
| | | Sends legal-terms webpage |
| | Activates and contacts its remote server for voting advice (how/which vote to manipulate) | |
| User accepts the legal terms | | |
| | | Sends start-voting page |
| Enters Initialisierungscode and date of birth, and submits them | | |
| | Extracts the Initialisierungscode and date of birth and stores it | |
| | | Validation of input, and sends the choose page |
| The user votes and submits them | | |
| | The plugin prevents the submission, extracts the user votes, modifies them according to the voting advice and submits it then (all within a few milliseconds) | |
| | At the same time, it sends the votes, together with identifying information such as the date of birth to the remote server (breaking voting secrecy) | |
| | | The server accepts the submission, and sends the review page |
| | The plugin modifies the HTML to match the votes to what the user entered before | |
| The user reviews and encrypts and submits the vote | | |
| | | The server sends the verify page |

| | | |
|---|---|---|
| | The plugin again modifies the votes to match what the voter voted for, and changes the verification scheme, including the explanatory texts to what we will discuss in detail below | |
| The user verifies the votes, enters the Bestätigungscode and submits the vote | | |
| | | The server accepts it, and delivers the confirmation page with the Finalisierungscode |
| The user checks it and ends the voting process | | |

* we are aware that switching between legal-terms, start-voting etc. is partially handled on the client side (AngularJS), for simplicity, we describe it as if it would be a classical side for simplicity reasons.

In the scheme above, first, we break voter secrecy by sending the votes to the remote server. Secondly, we can arbitrarily manipulate the votes without the voter knowing about it. Furthermore, as the requests are not modified and all the code submitted is as expected, the server can also not detect any manipulation.

For the above scheme, we have all required information available to interfere, except the verification codes for the votes we modify.

**How to handle this?**

We introduce a slightly modified verification scheme, which the user can very well expect to see there (it does not contradict the voting documents sent to them, or displayed.

Instead of showing the user all verification keys for the individual votes, we flip the verification and ask the voter to enter the verification code to check its correctness.

For all non-modified codes, we know the correct value, and thus we enforce the validation. As we expect that in a typical scenario, the third party is only interested in manipulating a limited number of the multiple initiatives for vote, this means that for almost all, the verification actually works as expected, i.e. the user has to enter the correct code, which gives them a lot of trust in the system.

For the manipulated votes, we still expect a four-digit input, we also add some time delay for the “verification execution” but label the code as correct, no matter what has been entered in the field. As most validations work as expected, it is safe to assume that this is not obviously happening at all, since

people stop testing after one or two failed inputs (we could even extend the scheme if people randomly try to fail all of them, to make this one fail as well).

**Optimizations**

Speed: We do not give the user a chance to spot any wrong inputs by directly switching from the input to displaying “verifying” after they entered the last digit.

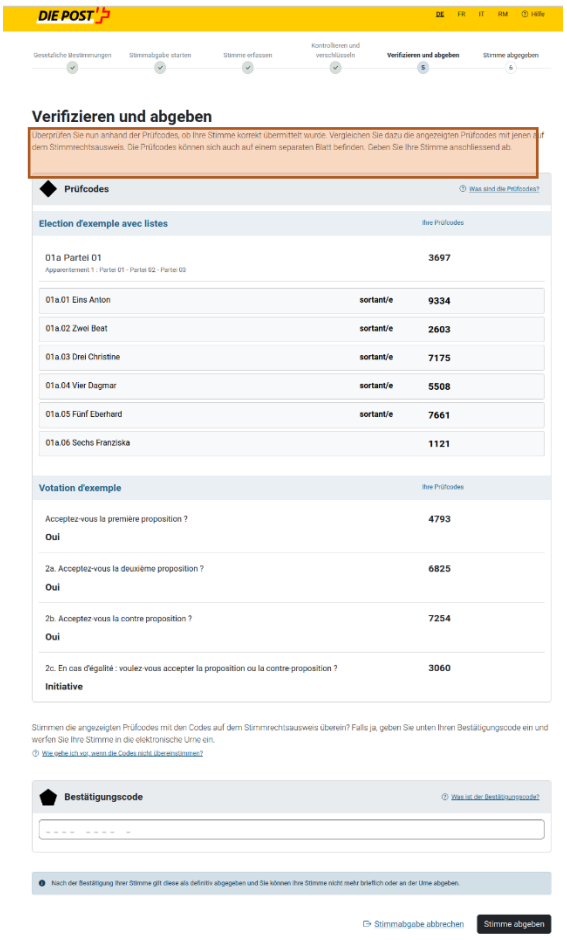
We ensure that the story is sound. For that, as you can see later below, we adjust all the information/description texts to match with our verification scheme.

We add a delay that feels natural compared to the other part of the web app, showcasing that we do some heavy crypto computation for their verification. In reality it is just a random time delay.

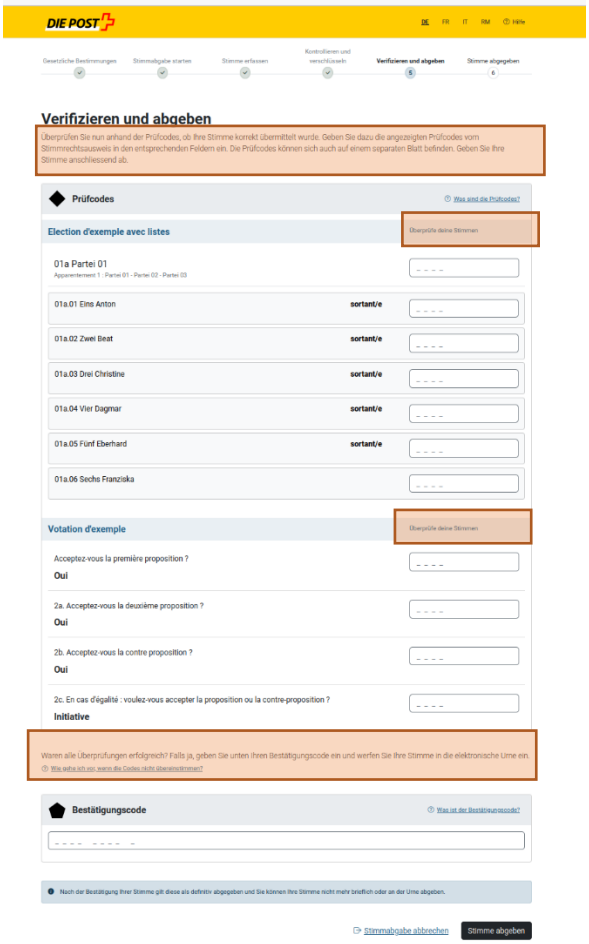
**Match with Text**

Furthermore, we included the voting documents from St.Gallen for the latest voting session, highlighting all relevant section for the verification. Looking at them showcases that our modified scheme, with the updated description text on the website does not raise obvious concerns or ambiguities.

**Original Verification**




**New Verification Scheme**




## User Testing

To check the schemes effectiveness, we conducted a mini study, asking a couple of people to run through this modified voting process. We provided the “Stimmrechtsausweis” and “Merkblatt für die elektronische Stimmabgabe”, and a set of the required codes to run through the voting (Initialisierungscode, Verifikationscodes, Bestätigungscode, Finalisierungscode). Furthermore, they were aware that something fishy is going to happen, tough their task was to find out what the problem is. They have never seen the voting platform before. Their background is a technical one, some of them even IT and software engineering, and all have a higher education degree (Bachelors, Masters from either a university or a polytechnic).

There were several inputs concerning the URL and the certificate (which of course are part of the test system), and the Swiss Post banner, which does not match my documents from St.Gallen. Furthermore, the banners “Please wait.. ” looked a bit weird to some of them (not as professional banners on other pages typically look like). However, none of them had a complaint about the verification scheme, which seemed to match well with the description on the webpage and the paper documents.

**Kanton St.Gallen**

P.P. CH-9001 St. Gallen | A-PRIORITY | Post CH AG

[redacted]

[redacted]

## Stimmrechtsausweis /
## Carte de vote /
## Carta di legittimazione di voto

**Erklärung:**
Ich stimme brieflich. Die Stimmabgabe entspricht meinem Willen.
Je vote par correspondance. Ce vote correspond à ma volonté.
Voto per corrispondenza. Il voto corrisponde alla mia volontà.

(eigenhändige Unterschrift/ signature manuscrite / firma autografa)

Kanton St.Gallen
Briefliche Stimmabgabe
Postfach 1640
9001 St.Gallen
SWITZERLAND

[redacted]

| Urnengang vom 18.06.2023 | Scrutin du 18.06.2023 | Votazione del 18.06.2023 |
|---|---|---|
| **Briefliche Stimmabgabe / Persönlich** | **Vote par correspondance / En personne** | **Voto per corrispondenza / Voto alle urne** |

- Unterschreiben Sie die Erklärung zur brieflichen Stimmabgabe auf diesem Stimmrechtsausweis.
- Legen Sie den Stimmzettel in das Stimmzettelkuvert und verschliessen Sie es.
- Legen Sie das verschlossene Stimmzettelkuvert und den unterschriebenen Stimmrechtsausweis in das Antwortkuvert, mit dem Sie das Stimmmaterial erhalten haben.
- Kontrollieren Sie, ob im Adressfenster die Rücksendeadresse erscheint.
- Übergeben Sie **das frankierte Antwortkuvert** rechtzeitig der Post. Antwortkuverts, die das Stimmbüro nicht bis zum Urnenschluss am Abstimmungstag erreichen, können nicht mehr berücksichtigt werden.

- Veuillez signer la déclaration de vote par correspondance sur la carte de vote.
- Veuillez glisser le bulletin de vote dans l'enveloppe électorale puis cacheter celle-ci.
- Veuillez glisser l'enveloppe électorale cachetée et la carte de vote signée dans l'enveloppe-réponse dans laquelle vous avez reçu le matériel de vote.
- Veuillez vérifier que l'adresse de renvoi apparaît dans la fenêtre prévue à cet effet.
- Veuillez poster **l'enveloppe-réponse affranchie** dans les délais. Les enveloppes-réponses parvenant au bureau de vote après la clôture du scrutin ne seront pas prises en compte.

- Firmare la dichiarazione relativa al voto per corrispondenza sulla presente carta di legittimazione di voto.
- Mettere la scheda di voto nella busta e chiuderla.
- Introdurre la busta chiusa con la scheda votata e la carta di legittimazione di voto firmata nella busta-risposta con la quale è stato recapitato il materiale di voto.
- Controllare che nella finestra l'indirizzo sia visibile.
- Inviare per tempo **la busta affrancata**. Le buste che giungono all'ufficio elettorale dopo la chiusura delle urne il giorno della votazione non possono più essere prese in considerazione.

Wollen Sie Ihre Stimme persönlich abgeben, teilen Sie dies bitte rechtzeitig dem Helpdesk mit.

Si vous désirez remettre votre bulletin de vote en personne, veuillez en informer le helpdesk à temps.

Se desiderate votare alle urne informatene l'helpdesk in tempo.

**E-Voting / Vote électronique / Voto elettronico**

Web-Adresse:
Adresse internet:
Indirizzo Internet: **https://sg.evoting.ch**

[redacted]

Initialisierungscode:
Code de initialisation:
Codice di inizializzazione: [redacted] ▲

Bestätigungscode:
Code de confirmation:
Codice di conferma: [redacted] ⬟

Finalisierungscode:
Code de finalisation:
Codice di finalizzazione: [redacted] ★

[redacted]

Die **elektonische Urne** öffnet am **22.05.2023 12:00:00** und schliesst am **17.06.2023 12:00:00 Uhr (Schweizer Zeit)**.
**L'urne électronique** ouvre le **22.05.2023 12:00:00** et ferme le **17.06.2023 12:00:00 (heure suisse)**.
**L'urna elettronica** apre il **22.05.2023 12:00:00** e chiude il **17.06.2023 12:00:00 (ora svizzera).**

[redacted]

**Helpdesk:** Montag - Freitag 08:00 Uhr - 11:30 Uhr und 14:00 Uhr - 17:00 Uhr, Tel.: +41 58 229 88 88, E-Mail: evoting@sg.ch
**Helpdesk:** Du lundi au vendredi, de 08h00 à 11h30 et de 14h00 à 17h00, Tél.: +41 58 229 88 88, courriel: evoting@sg.ch
**Helpdesk:** lunedì - venerdì dalle 08.00 alle 11.30 e dalle 14.00 alle 17.00, Tel.: +41 58 229 88 88, indirizzo mail: evoting@sg.ch

Die unbefugte oder mehrmalige Teilnahme an einer Wahl oder Abstimmung ist als Wahlfälschung strafbar (Art. 282 StGB).
Participer à une élection ou à une votation sans y être autorisé ou à plusieurs reprises est punissable en tant que fraude électorale (art. 282 CP).
Chi partecipa a un'elezione o a una votazione senza averne il diritto o vi partecipa più volte è punibile per frode elettorale (art. 282 CP).

Alle nachfolgenden Angaben dienen der Sicherheit von E-Voting. Wir empfehlen Ihnen, von diesen Kontrollelementen Gebrauch zu machen. Bitte wenden Sie sich an den Helpdesk, wenn falsche Codes angezeigt werden oder andere Prüfungen ein negatives Ergebnis aufweisen.
Tous les éléments suivants servent à vérifier la sécurité du vote électronique. Nous vous recommandons de faire usage de ces éléments de contrôle. Merci de prendre contact avec le Helpdesk si de mauvais codes sont affichés ou si d'autres contrôles affichent un résultat négatif.
Tutti i seguenti elementi servono per verificare la sicurezza del voto elettronico. Vi raccomandiamo di utilizzare questi elementi di verifica. Contattare l'Helpdesk in caso di codici di test visualizzati in modo errato o di ulteriori test con risultati negativi.

Wichtige Informationen zum Vorgehen und zur Verwendung der Prüfcodes finden Sie auf der Webseite des Kantons: https://e-voting.sg.ch. Im Fall von widersprüchlichen Angaben halten Sie sich bitte an die Informationen auf dem Stimmrechtsausweis, und nicht an die Informationen, die auf Webseiten angezeigt werden.
Des informations importantes sur les codes de vérification peuvent être consultées sur la page internet du canton: https://e-voting.sg.ch. En cas de doute, nous vous demandons de vous en tenir aux informations de la carte de vote et non à celles qui sont affichées sur les pages Internet.
Informazioni importanti sulla procedura e sui codici di verifica sono disponibili sul sito web del Cantone: https://e-voting.sg.ch. In caso di dubbio, è bene attenersi alle informazioni presenti sulla scheda di voto e non a quelle delle pagine Internet.

**Fingerprint (SHA-256) des Zertifikats von https://sg.evoting.ch:**
**Empreinte numérique (SHA-256) du certificat de https://sg.evoting.ch:**
**Impronta digitale (SHA-256) del certificato da https://sg.evoting.ch:**

C2 8C 67 EA E4 93 0B 94 46 01 5A C6 9F EF 13 77 76 35 6F 0B
82 34 6A E8 A9 5E E5 61 F4 7E 25 FC

**Prüfcodes / Codes de vérification / Codici di verifica** ◆

**Eidgenössische Volksabstimmung vom 18.06.2023 / Votation populaire fédérale du 18.06.2023 / Votazione popolare federale del 18.06.2023**

| | | | |
|---|---|---|---|
| Vorlage 1 / Objet 1 / Oggetto 1 | Ja / Oui / Sì [redacted] | Nein / Non / No [redacted] | Leer / Blanc / Bianco [redacted] |
| Vorlage 2 / Objet 2 / Oggetto 2 | Ja / Oui / Sì [redacted] | Nein / Non / No [redacted] | Leer / Blanc / Bianco |
| Vorlage 3 / Objet 3 / Oggetto 3 | Ja / Oui / Sì [redacted] | Nein / Non / No [redacted] | Leer / Blanc / Bianco |

**Kanton St.Gallen**
**Staatskanzlei**

# Merkblatt für die elektronische Stimmabgabe

## Guide pour le vote électronique / Istruzioni per il voto elettronico

Der Stimmrechtsausweis enthält Ihre persönlichen Zugangsdaten für die elektronische Stimmabgabe. Bitte gehen Sie sorgfältig damit um und halten Sie ihn bis zum Abschluss des Urnengangs unter Verschluss.

La carte de vote contient vos données d'accès personnelles pour le vote électronique. Veuillez en prendre soin et le garder de manière confidentielle jusqu'à la clôture du scrutin.

La carta di legittimazione contiene i dati personali di accesso al voto elettronico. Si prega di maneggiarla con cura e di tenerla sotto chiave fino alla chiusura delle urne.

**1**

### Aufrufen / appeler / accedere https://sg.evoting.ch

Bitte berücksichtigen Sie die technischen Sicherheitshinweise.

Veuillez tenir compte des consignes de sécurité techniques.

Osserva le istruzioni tecniche di sicurezza.

**2** ▲

### Starten / lancer / lanciare

Initialisierungscode und Geburtsdatum eingeben.

Saisir le code d'initialisation et la date de naissance.

Inserisce il codice di inizializzazione e la data di nascita.

**3**

### Abstimmen / voter / votare

Stimme abgeben oder leer lassen.

Voter ou laisser vide.

Esprime il suo voto o lasciatelo vuoto.

**4** ◆

### Vergleichen / comparer / confrontare

Sind die Prüfcodes auf dem Portal und auf dem Stimmrechtsausweis identisch? Bitte wenden Sie sich an den Helpdesk, wenn falsche Codes angezeigt werden.

Les codes de vérification sur le portail et la carte de vote sont-ils identiques? Voulez-vous adresser au support si des codes erronés sont affichés.

Sono identici i codici di verifica sul portale e sulla carta di legittimazione? Contatta l'helpdesk se vengono visualizzati codici errati.

**Helpdesk E-Voting**
Montag bis Freitag 08.00 Uhr - 11.30 Uhr und 14.00 Uhr - 17.00 Uhr
Tel. +41 58 229 88 88
E-Mail evoting@sg.ch

## 5 ⬟ Bestätigen / confirmer / confermare

Bestätigungscode eingeben, wenn alle Prüfcodes übereinstimmen.
Geben Sie Ihren Bestätigungscode nicht ein, so wird Ihre Stimme nicht in die elektronische Urne eingeworfen. In diesem Fall können Sie Ihre Stimme weiterhin brieflich oder an der Urne abgeben.

Saisissez le code de confirmation si tous les codes de vérification correspondent. Si vous ne saisissez pas votre code de confirmation, votre vote ne sera pas déposé dans l'urne électronique. Dans ce cas, vous pouvez continuer à voter par correspondance ou à l'urne.

Immette il codice di conferma se tutti i codici di verifica corrispondono.
Se non si inserisce il codice di verifica, il voto non verrà inserito nell'urna elettronica. In questo caso, è ancora possibile esprimere il proprio voto per posta o al seggio.

## 6 ★ Abschliessen / conclure / concludere

Ist der Finalisierungscode auf dem Portal mit jenem auf dem Stimmrechtsausweis identisch? Bitte wenden Sie sich an den Helpdesk, wenn falsche Codes angezeigt werden.

Le code de finalisation est-il identique sur le portail et sur la carte de vote? Veuillez contacter le support si des codes erronés sont affichés.

Sono identici i codici di finalizzazione sul portale e sulla carta di legittimazione? Contatta l'helpdesk se vengono visualizzati codici errati.

**Helpdesk E-Voting**
Montag bis Freitag 08.00 Uhr - 11.30 Uhr und 14.00 Uhr - 17.00 Uhr
Tel. +41 58 229 88 88
E-Mail evoting@sg.ch

**Test System vs Production System**

In the E2E Gitlab repo, there is a disclaimer showcasing essential security concepts that are omitted in the test system. In this section, we argue that these systems cannot prevent our attack.

*"[…] The development environment does not represent Swiss Post's productive environment and omits numerous security elements such as HTTP security headers, separate network zones, and a web application firewall."*

https://gitlab.com/swisspost-evoting/e-voting/evoting-e2e-dev/-/tree/evoting-e2e-dev-1.3.0.0

(1) HTTP security headers such as X-XSS-Protection, Strict-Transport-Security (HSTS) or Content-Security-Policy (CSP) could indeed potentially interfere with such an extension, especially considering that we communicate with a remote server (voting advice and sending of the user votes).

As a Firefox extension however, we can modify all request and response headers on the fly before the HTML is interpreted and the JavaScript is executed, thus making these headers void. We did not integrate it into our PoC extension, but to showcase the feasibility, you can find the "modheader-firefox" addon that exactly does this: https://addons.mozilla.org/en-US/firefox/addon/modheader-firefox/

(2) Separate network zone do not prevent or influence our attack, as the extension runs on in the client's browser

(3) A web application firewall cannot prevent this attack, as the requests and responses are unmodified and thus legitimate.

**Security Elements**

With this attack, all the security elements are still intact. Namely the SSL/TLS certificate and the Javascript library hashes, which makes this attack hard to detect.

Furthermore, we simply omitted to add an icon for the extension, which leads to the extension not being shown in the browser taskbar. Thus it is completely hidden from the user. The only chance to see it is actively clicking on the "Extensions" button, though the plugin could be hidden as part of another useful browser extension such as an adblocking extension or a free VPN.

**Limitation of the PoC**

Implementing such a plugin requires a lot of programming efforts, in this case over 500 lines of code. Thus, certain aspects that do not reduce the expressiveness of the PoC have been simplified to reduce the programming burden. Namely:

- Even though the voting contains different parts, namely the vote for parties and people, as well as a yes/no/blank part for initiatives. The current PoC only modifies the four initiatives but could be easily extended for the other parts of the vote.
- The default setting of the E2E deployment uses inconsistent language (parts are in French, others are in German, ..). We kept it and adjusted the PoC accordingly to fit in best (i.e. the modification of the answers are in the language they were on the non-modified page, namely in French)
- We hardcoded the XPATHs that define the DOM element that needs to be modified. A different vote or different version of the platform would potentially need to be slightly adjusted to meet the new structure.
- The new verification scheme is no production code. It works as intended, but there might be some uncaught side conditions for the validation, as I did not extensively test and optimize it.

**Conclusion**

With the attack described above we can view the user vote (voting secrecy), play a valid vote process for the user, while in the background submitting valid, but manipulated votes.

All of this is possible under the sole assumption that the voting system has to guarantee individual verifiability, even in case of a virus on the user device (our virus is the web browser plugin, running in the background), as described in the explanatory report, section 4.2.1

**Proof of Concept - Video**

To simplify the understanding of how this system works, not only provide the code for the proof of concept, but also a demonstration in the form of a video that runs through the process.

Video the way the user would encounter this:

*[link + password to the video, redacted]*

Video with demonstration and comments on what is happening under the hood:

*[link + password to the video, redacted]*

**Proof of Concept – Code**

The proof of concept consists of a browser plugin, specifically crafted for the latest version of Firefox. The plugin can be loaded as follows:

1) Open Firefox
2) Enter “about:debugging#/runtime/this-firefox” in the status bar and press enter
3) Load temporary plugin -> select manifest.json

Setting the variable “demo” in the header of main.js from false to true allows to display a lot of intermediate debug messages.

Furthermore, we have a Python/Flask-based web application for the remote server, delivering the voting advice and accepting the user votes to store.

**System Details:**

Host computer: Ubuntu 22.04 / Firefox 111.0.1

The e-voting platform (version 1.3.0.0) has been built and deployed according to the e2e documentation found on GitLab:

- Building Guide: https://gitlab.com/swisspost-evoting/e-voting/e-voting/-/blob/master/BUILDING.md
- Running: https://gitlab.com/swisspost-evoting/e-voting/evoting-e2e-dev
- Run election event (using the default parameters): https://gitlab.com/swisspost-evoting/e-voting/evoting-e2e-dev/-/blob/master/docker-compose/Run_Election_Event.md

The PoC code can be downloaded here:

*[link + password to the PoC code, redacted]*

## Remedies

I feel that the only true solution to solving the issue would need a secure boot / attestation and running signed software only. Though, there are a couple of remedies that would improve overall security and reduce the risk, while keeping usability in mind.

### Improvement of the Info Sheet

The verification is an integral part of the whole voting process, if not the most important step from a voter's perspective! The exact procedure, including a screenshot of how this should look like has to be included very prominently on the info sheet.

### Clean browser

A clean/fresh installed browser would mitigate this attack. This could be delivered via a USB flash drive as part of the voting material. Such a delivery would further allow to strengthen the protection mechanisms, for example by including features such as a VPN tunnel or a TOR connection to obfuscate/hide the voting to protect users in foreign countries. Furthermore, this browser could be locked down to prevent extensions from being executed.

### Private Session

Encouraging the voter to run their voting in a private browsing session would not only increase security against this attack, but actually in general (cookies, ..), as most browser extensions for example are disabled by default in private browsing, and depending on the browser, additional anti-tracking measures are in place.

### Javascript-based Fraud Detection

As part of the web app, a Javascript-based agent could be included that checks for interferences or modification of the HTML DOM throughout the voting process and immediately report any sort of manipulation. Though, this is a cat-and-mouse game, as the script could be disabled using an extension prior to HTML DOM modification.