Voatz

Responses & Comments for (Trail of Bits Report)

[Version 1.0 - Last updated: May 10, 2020

1. Status & Mitigations

Our responses and comments to the list of issues reported by Trail of Bits in March 2020 are listed below. The Voatz security team evaluated each issue over multiple iterations to determine its status and relevance.

Issue Type	***Reported***	***Resolved***	***Not Relevant***	***False Positive***	***Partially Addressed***
High Severity [H]	16	9	1	6	0
Medium Severity [M]	12	5	2	3	2
Low Severity [L]	10	6	2	2	0
Undetermined Severity [U]	6	0	2	4	0
Informational Severity [I]	4	0	2	2	0
	48	***20***	***9****	***17*****	***2***

**Not Relevant – indicates that, upon further testing by the Voatz security teams, the issue was found to be non-applicable due to code deprecation or a misunderstanding of the functionality.*
***False Positive – indicates that, upon further testing by the Voatz security teams, the issue was found to be not practically exploitable due to other mitigations or safeguards in place.*

<u>1. TOB-VOATZ-014 (Device IDs not validated against inner request device IDs)</u>
For endpoints that are sensitive, Voatz believes that the additional session management checks in place in the code provide sufficient protection against such a threat. For endpoints that are not sensitive, there is no risk to a transaction and Voatz believes based on the testing that the various layered security protocols already detect misuse. [H]
Status – False Positive.

<u>2. TOB-VOATZ-017 (Amazon admin password)</u>
This unused test code has been removed from the repository. Regardless, this code would have had no impact whatsoever on a live election infrastructure. [H]
Status – Resolved.

<u>3. TOB-VOATZ-016 (Ballot receipts for non-secret ballot election types)</u>
This functionality was last used in a non-secret ballot election in 2018 and has since been deprecated. We don't believe it is relevant at all to public elections. [H]
Status – Not Relevant.

<u>4. TOB-VOATZ-013 (Secrets stored as environment variables)</u>
Voatz believes that its internal controls already provide sufficient safeguards to prevent misuse. Variables are immediately cleared to prevent any kind of misuse. [H]
Status – False Positive.

<u>5. TOB-VOATZ-010 (API for cloud onboarding workflow)</u>
This is an incorrect observation. Voatz uses project specific cloud buckets wherever necessary and appropriate cleanups are performed. Voatz plans to address scalability challenges as part of the version 2 of its platform. [H]
Status – False Positive.

<u>6. TOB-VOATZ-020 (Receipt and affidavit filename collisions)</u>
This was mitigated by implementing single-use audit tokens that cannot be reused again. [H]
Status – Resolved.

<u>7. TOB-VOATZ-022 (A voter can unregister another voter's device)</u>
This has been addressed by permanently enforcing the relevant parameter value. [H]
Status – Resolved.

8. TOB-VOATZ-023 (Input material for AESGCM sent to Graylog)
This code has been removed. [H]
Status – Resolved.

9. TOB-VOATZ-028 (Voatz backend SSL key has a subdomain wildcard)
Voatz uses dynamic subdomains for security and has multiple wildcard certificates for redundancy with its keys being well protected. Voatz doesn't see any need to change this at this time. [H]
Status – False Positive.

10. TOB-VOATZ-046 (Clients can specify their own audit token)
Voatz believes the other controls in place (such as single use audit tokens) in the system provide sufficient safeguards to prevent misuse if a malicious actor were to attempt this. [H]
Status – False Positive.

11. TOB-VOATZ-047 (Test parameters in the registration APIs)
This test code has been removed from the repository. Regardless, this code would have had no impact whatsoever on a live election infrastructure. [H]
Status – Resolved.

12. TOB-VOATZ-009 (QR code generation for large non-secret ballot cases)
This test code has been removed from the repository. This functionality was last used in a non-secret ballot election in 2018 and has since been deprecated. We don't believe it was relevant at all to public elections. [M]
Status – Resolved.

13. TOB-VOATZ-018 (Session timeout validation)
This finding is not relevant. A memcached session entry is ejected when the TTL or TimeToLive expires. This setting is configurable server side and is used to control the duration of a valid session. This renders the MaxIdleTime setting superfluous and it is for this reason the code reading the MaxIdleTime setting was commented out. [M]
Status – Not Relevant.

14. TOB-VOATZ-015 (Receipt encryption is weak)
Voatz has made improvements to this as part of its newer releases. [M]
Status – Pending, Partially Resolved.

15. TOB-VOATZ-019 (Insufficient device ID validation)
Voatz has added good-form validation and increased the length of device IDs as part of its newer releases to avoid this issue. [M]
Status – Resolved.

16. TOB-VOATZ-035 (Potential resource exhaustion)
Voatz believes its layered security protocols currently detect this at an early stage and stop any potential misuse. [M]
Status – False Positive.

17. TOB-VOATZ-030 (Resource exhaustion)
Voatz believes its layered security protocols already detect this at an early stage and stop any misuse. [M]
Status – False Positive.

18. TOB-VOATZ-029 (Zimperium checks)
Voatz believes that its 3-way off channel check will detect attempts to bypass Zimperium as such a check is not visible to an attacker. This security mechanism has been validated in several elections conducted this year. [M]
Status – False Positive.

19. TOB-VOATZ-024 (AES-GCM key/nonce/tag breaks authenticity)
This has been addressed as part of the fix for TOB-VOATZ-011. [M]
Status – Resolved.

20. TOB-VOATZ-004 (Unauthenticated ECDH)
This is being addressed as part of a new protocol implementation in v2 and is not immediately relevant due to other controls in place on the server side. [M]
Status – Pending, Partially Addressed.

21. TOB-VOATZ-011 (AES-GCM key/nonce/tag are encrypted with AES-ECB)
This has been addressed by replacing the lone usage with AES-GCM. [M]
Status – Resolved.

22. TOB-VOATZ-033 (OSCP Stapling)
This has been enabled on the relevant Voatz servers. [M]
Status – Resolved.

23. TOB-VOATZ-027 (Empty ballots are not recorded)
Voatz has addressed this in the audit documentation. [L]
Status – Resolved.

24. TOB-VOATZ-016 (Database root credentials)
These were old local test credentials from a few years ago and are no longer used. Regardless, these would have had no impact whatsoever on a live election infrastructure. [U]
Status – False Positive.

25. TOB-VOATZ-021 (Signed voter affidavits are sent to an administrative email)
This finding is not relevant. Firstly, this is required per the legal guidelines of the election jurisdictions. See sample affidavit for reference. Secondly, the destination email is provided by the jurisdiction. The email address in your snippet is just a placeholder. Thirdly, our pilot jurisdictions already allow eligible absentee voters to return ballots via email or efax (~remember Voatz is an additional method that is being piloted) and have their own practices, procedures in terms of handling spam, etc. Lastly, Voatz servers send these emails from a whitelisted email address using a dedicated IP address and using a service that is protected using DMARC, DKIM, SPF. [U]
Status – Not Relevant.

26. TOB-VOATZ-012 (AES-GCM AAD usage is non-standard)
Voatz is comfortable with its AAD usage and believes that our approach actually aids its layered defense protocols. [U]
Status – False Positive.

27. TOB-VOATZ-005 (Session cookie offset)
This is not a relevant finding. There is no practical risk to using these offsets that are updated periodically. [I]
Status – Not Relevant.

28. TOB-VOATZ-048 (Encrypted application data is brute forceable)
This was resolved by changing the application functionality to use encrypted shared preferences based secured persistent storage on Android. [H]
Status – Resolved.

29. TOB-VOATZ-025 (PDKF2 provides insufficient security)
This has been addressed as part of the updates for TOB-VOATZ-048. [H]
Status – Resolved.

30. TOB-VOATZ-032 (Third party apps capture)
This has been addressed by adding the relevant flag. [H]
Status – Resolved.

31. TOB-VOATZ-003 (Android release build signing keys)
Voatz believes the frequent key rotation, other controls in place provide sufficient safeguards. [H]
Status – False Positive.

32. TOB-VOATZ-035 (Malicious website can read internal storage)
This has been addressed by enabling the relevant flag. [H]
Status – Resolved.

33. TOB-VOATZ-008 (Insufficient Android device ID construction)
This was addressed as part of the earlier fix. The reregistration upon device reset is a mandatory part of the user workflow and users are advised about the same via help messages, other tutorials. [L]
Status – Resolved.

34. TOB-VOATZ-037 (Android client doesn't use SafetyNet Attestation API)
This has been addressed as part of the newer releases earlier this year. [L]
Status – Resolved.

35. TOB-VOATZ-045 (Android client doesn't use SafetyNet Verify API)
This has been addressed as part of the newer releases earlier this year. [L]
Status – Resolved.

36. TOB-VOATZ-026 (Certificate pinning is only configured for main domain)
This impacts non-Voatz components only. Voatz had requested the relevant third parties to address this issue and they have addressed it as part of their newer releases. [L]
Status – Pending, Partially Addressed.

37. TOB-VOATZ-034 (No explicit verification of Android security provider)
This is already addressed via the Zimperium integration. [L]
Status – False Positive.

38. TOB-VOATZ-001 (Jumio Netverify API credentials stored in git)
These were a few years old and have since been rotated and are no longer stored in git. Regardless, this would have had no impact whatsoever on a live election infrastructure. [L]
Status – False Positive.

39. TOB-VOATZ-002 (Google Services API key stored in git)
This file has been removed from the repository. [U]
Status – Resolved.

40. TOB-VOATZ-036 (Malicious website can execute javascript within the Android client)
This was initially deemed relevant but upon further investigation, it was revealed the websites served inside the mobile application are specifically whitelisted and specially curated (e.g. blue books, etc.). [I]
Status – False Positive.

41. TOB-VOATZ-040 (iOS client doesn't disable custom keyboards)
Custom keyboard support is required for accessibility and Voatz doesn't see any undue risk here as manually typing requirements are very limited in the application anyway. [M]
Status – Not Relevant.

42. TOB-VOATZ-042 (iOS client doesn't use system managed login input fields)
Voatz doesn't use standard login inputs due to the biometrics so this finding is not relevant. [L]
Status – Not Relevant.

43. TOB-VOATZ-043 (iOS keychain items)
Voatz has addressed this in its newer releases. [L]
Status – Resolved.

44. TOB-VOATZ-041 (Cryptographic credential generation)
This was resolved as part of the iOS 13 upgrades. However, there are certain iOS devices that cannot be upgraded beyond iOS 12.4.4 and additional safeguards are available for those as an alternative. [L]
Status – Resolved.

45. TOB-VOATZ-044 (iOS client disables ATS)
This is not a relevant finding. This is required for mobile threat defense and to support the Zimperium integration. [L]
Status – Not Relevant.

46. TOB-VOATZ-038 (iOS client is vulnerable substitution attacks)
This impacts only the non-Voatz components and cannot be used to affect an internal transaction. Voatz has already informed the 3rd parties who have addressed with additional mitigations on their end. [U]
Status – Resolved.

47. TOB-VOATZ-007 (iOS user can lose registration)
This is intentional and designed for security. It is similar to TOB-VOATZ-008 wherein the Android reregistration is enforced. [I]
Status – Not Relevant.

48. TOB-VOATZ-039 (iOS client is susceptible to URI scheme hijacking)
Voatz confirms that it is not using the URI scheme for any purposes. [I]
Status – False Positive.

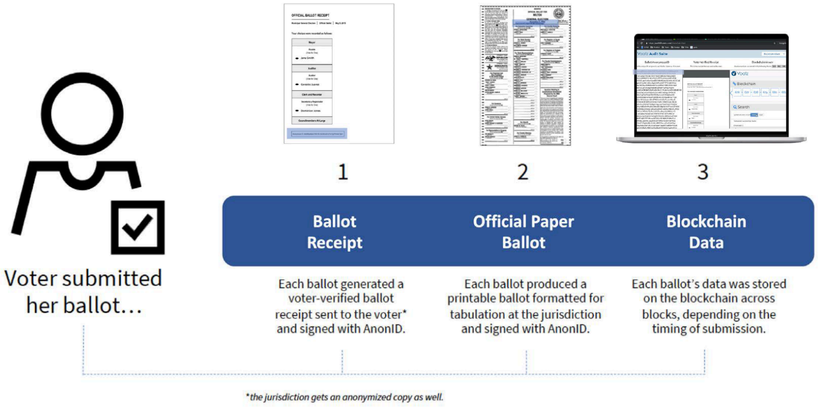
2. Security by Design

Security has been at the forefront of the Voatz solution architecture since the very beginning, including the company's earliest roots in winning first prize at the 2014 SXSW hackathon. The founders continue to believe that security must sit at the heart of the company's design principles, and the technology's development closely follows this thesis.

The architecture of the Voatz solution sits on hardware and software designed to provide platform security. This security architecture spans all devices, servers, and networks used by the Voatz solution and incorporates device verification, real-time mobile threat detection and mitigation, remote identity proofing, distributed ledger-based data security, and a user-centric approach to end-to-end vote verification. Inherent in the Voatz culture is the philosophy of continuous improvement. Voatz management and shareholders require regular third-party evaluations, daily security testing, and constant enhancements in the presence of real-world threats, all aimed to supplement and continuously strengthen this architecture.

Core security tenets at the heart of the Voatz technology

All layers of the system enable an end-to-end process to ensure that all ballots are counted as intended and verified by the voter: (1) The platform produces a paper ballot for the jurisdiction to tabulate; (2) The system automatically sends the voter a password-protected, anonymized ballot receipt; and (3) The system uses a blockchain-based, tamper-resistant ledger to secure the aggregate vote and enable rigorous post-election audits.



Each ballot generated a voter-verified ballot receipt sent to the voter* and signed with AnonID.

Each ballot produced a printable ballot formatted for tabulation at the jurisdiction and signed with AnonID.

Each ballot's data was stored on the blockchain across blocks, depending on the timing of submission.

*the jurisdiction gets an anonymized copy as well.

Diagram showing the multiple ballot trails generated by every mobile ballot submission, which facilitate a robust post-election audit

These checks and balances ensure that every single voter can verify their vote, that every election official can tabulate a paper ballot, and that the stakeholders involved in the election process can audit the integrity of the overall count without revealing voter identity.

2.1 How Mobile Voting Works

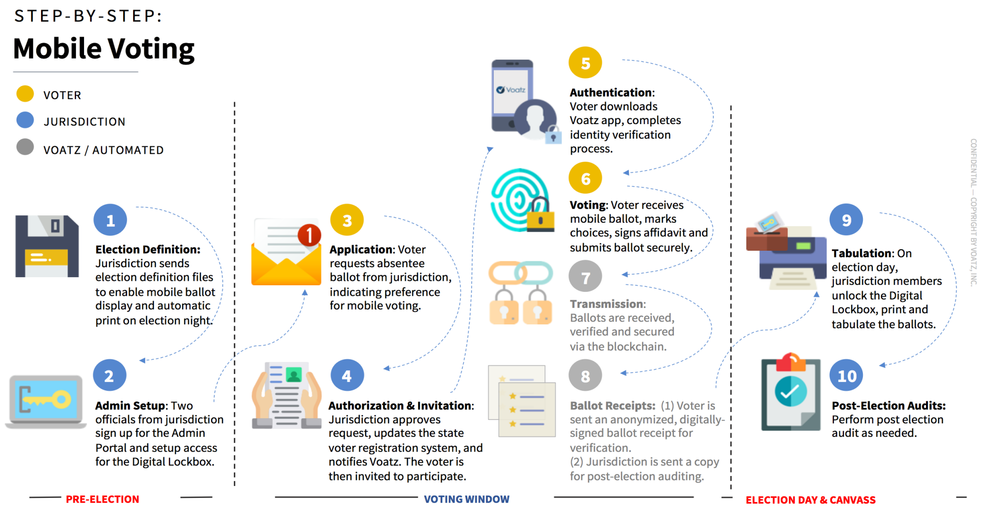
Voatz offers a new channel of voting within the traditional voting landscape. If a voter cannot vote in-person at the polls, early nor by mail, they have a fourth option: mobile voting.

Across its voting platform, Voatz leverages the latest smartphone security features and pairs them with multifactor authentication, including biometrics and facial recognition technology, to verify and validate the identity of the voter. The voter experience is seamless: 1) sign up to "vote mobile" on your absentee request form; 2) download the app and verify your identity; and 3) vote.

Privacy and security are inherent in the design of the Voatz solution. As soon as the voter's identity is verified, all identifying documents are deleted, and the voter's identity is anonymized.

The voter immediately receives a ballot receipt to verify their selections. A record of the marked ballot is written to the blockchain to assure data security and support the post-election audit process. Finally, a paper ballot is produced for the jurisdiction to tabulate alongside ballots received via the traditional voting methods.

At the close of every election, the jurisdiction has the option to host an open, public audit of all electronic ballot submissions. Any citizen can sign up to be an auditor. These auditors gain access to an audit portal with each mobile ballot submission's paper ballot, their anonymized ballot receipt, and the data on the blockchain. These audits are amongst the first in history to be fully open and transparent. This expansion of the audit process is part of an ongoing effort to widen a community of stakeholders, to build trust, and foster integrity in our critical infrastructure.



STEP-BY-STEP:

Mobile Voting

● VOTER

● JURISDICTION

● VOATZ / AUTOMATED

1 **Election Definition:** Jurisdiction sends election definition files to enable mobile ballot display and automatic print on election night.

2 **Admin Setup**: Two officials from jurisdiction sign up for the Admin Portal and setup access for the Digital Lockbox.

3 **Application**: Voter requests absentee ballot from jurisdiction, indicating preference for mobile voting.

4 **Authorization & Invitation**: Jurisdiction approves request, updates the state voter registration system, and notifies Voatz. The voter is then invited to participate.

5 **Authentication**: Voter downloads Voatz app, completes identity verification process.

6 **Voting**: Voter receives mobile ballot, marks choices, signs affidavit and submits ballot securely.

7 **Transmission**: Ballots are received, verified and secured via the blockchain.

8 **Ballot Receipts:** (1) Voter is sent an anonymized, digitally-signed ballot receipt for verification. (2) Jurisdiction is sent a copy for post-election auditing.

9 **Tabulation**: On election day, jurisdiction members unlock the Digital Lockbox, print and tabulate the ballots.

10 **Post-Election Audits:** Perform post election audit as needed.

How Voatz works for a voter and how the system integrates with a jurisdiction

2.2 Election Industry Innovations Pioneered by Voatz

A comprehensive list of innovations in the Voatz platform includes:

- Native smartphone applications for highly accessible (ADA regulation compliant) remote ballot delivery, marking and return
- Remote identity proofing of voters using government-issued photo IDs paired with cutting-edge liveness and facial recognition technology
- Auditable, automated, fully-marked and formatted paper ballot generation for each mobile vote for tabulation
- Remote ranked-choice voting using an accessible interface

- Use of distributed ledger technology to secure the aggregate vote and enable post-election audits
- Real-time mobile threat detection and mitigation
- Visual and voter-centric approach to citizen-led post-election audits
- Coercion detection capabilities
- Public bug bounty programs and continuous third-party security assessments as input to Voatz's continuous improvement philosophy

2.3 Defense in Depth

The Voatz platform incorporates the security principle of *Defense in Depth.* There are multiple layers of security controls deployed across the platform, each approaching risk in different ways to build layers of defense around each asset.

Some key examples include our approach to remote identity proofing to determine voter eligibility, mobile device threat detection, and mitigation, botnet attack mitigation, etc.

2.4 A Model Based on Continuous Improvement

Voatz has been committed to the process of continuous improvement since its inception. The company conducted its very first white box, third party security assessment in 2016, and continues to pursue examinations of this kind since. In 2019, Voatz voluntarily submitted its platform to CISA (under the U.S. Department of Homeland Security) for an infrastructure security assessment (HUNT). In 2020, Voatz pursued a critical product evaluation (CPE) and continues to work with relevant private cybersecurity assessment firms for additional testing and evaluation.

Assessments of this kind are essential to the pursuit of continuous improvement as Voatz works to stay ahead of ever-evolving cyber threats. Any relevant issues detected during these audits are triaged and resolved promptly, or mitigated as needed. Recently, Voatz became the first mobile voting solution to successfully undergo a comprehensive assessment by a federally certified VSTL (Voting Systems Test Laboratory). Phase 1 was completed in May 2020, and Phase 2 was completed in July 2020.

Voatz has been the subject of intense media scrutiny and criticism by some security academics who have attempted to break into the system unsuccessfully on multiple occasions. Despite these attempts, Voatz remains the most battle-tested remote voting platform, has never had a successful security breach, nor experienced any voter fraud, and has thwarted every break-in attempt. In a recent election involving thousands of voters, the Voatz platform detected and prevented an unprecedented number of advanced mobile device threats in real-time, including insecure wireless networks, to fully ensure the integrity of the electoral process.

3. About Us

3.1 Team & Advisors

The Voatz team includes experts spanning mobile security, high-performance SaaS, product design, election systems management and certifications, financial technology, and beyond. It is due to this unique blend of expertise that Voatz has managed to maintain and press forward with progress in the space.

IBM
Carnegie Mellon University
Clear Ballot
AMERICAN EXPRESS
PEACE CORPS
Lotus
IDEO
EUROPAY International
accenture
IDEMIA augmented identity
WELLS FARGO ADVISORS
fido ALLIANCE simpler stronger authentication
IT University of Copenhagen
SMARTMATIC

- Mobile security
- Network security
- Digital payments and identity
- High performance SaaS systems
- Election systems administration
- Accessible product design

The Voatz Advisory Board includes eminent professionals with sector expertise spanning elections, cybersecurity, nation-state threat mitigation, financial technology, politics, government, civic innovation, and business.

INVEST | AMERICA
AMERICANS·ELECT
HARVARD Kennedy School JOHN F. KENNEDY SCHOOL OF GOVERNMENT
Clear Ballot
Lotus
Walt Disney IMAGINEERING
CNN
HARVARD Kennedy School JOHN F. KENNEDY SCHOOL OF GOVERNMENT
EMVCo
fido ALLIANCE
AM EX
accenture
CORI Center on Rural Innovation

Kahlil Byrd
Political Strategist, Expert on Cross Partisan Political Reform

Larry Moore
Elections Industry Expert, Ex-CEO of ClearBallot

Eric Haseltine
Futurist, Author, Neuroscientist, Intelligence Officer

Juliette Kayyem
Ex-Homeland Security, Resilient Infrastructure Expert, CNN National Security Analyst

Philip Andreae
Payments & FinTech Security Expert

Shannon O'Brien
1st Female Treasurer of MA, Gubernatorial Candidate, Evangelist

Matt Dunne
VT Legislator, Ex-Director of AmeriCORPs, Center for Rural Innovation

3.2 Investors & Awards

A committed group of investors backs Voatz's focus on next-generation technologies, blockchain, and civic innovation. The company is a graduate of both the Techstars Boston 2017 and MassChallenge Boston 2017 startup accelerator programs and has raised an aggregate of $9.2 million across two rounds of venture funding. Voatz is also the winner of several technical, civic innovation awards, including the MassChallenge 2017 Gold Award Winner, Microsoft Civic Innovation Award 2017, Election Center's Democracy Award (Denver County) 2019, Innovative Entrepreneurship in Blockchain Award (Public Sector Services) 2019, and was a finalist at the GSMA Mobile World Congress 2020 Awards for Best Mobile Innovation for Accessibility and Inclusion.