

 BRIEF

U.S. MIDTERM ELECTION SERIES: VOTING MACHINE SECURITY ZEROFOX INTELLIGENCE

B-2022-10-10a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Elections Infrastructure

October 10, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 5:00 PM (EDT) on October 6, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

U.S. Mid-term Elections Series: Voting Machine Security

Executive Summary

The integrity of votes cast in U.S. elections has come under increased scrutiny in recent years, with partisans of both major political parties calling the outcomes of high-visibility races into question over allegedly-flawed processes.¹² While investigations to date have not yielded evidence of malicious actors decisively altering voter registration records or voting results,³ vulnerable practices and technology have been identified in a number of voting systems. Most identified vulnerabilities can be addressed, if not prevented, through a combination of physical and digital access controls, timely software patching, and consistent “air-gapping” of systems. The security practices of individual states administering election systems are not always evident, however, indicating some vulnerability in the U.S. electoral process as a whole.

Election systems have numerous sensitive components, including voter registration databases, electronic polling books, voting machines, and ballot scanners. The scope of this report is limited to voting equipment used at polling locations and ballot-counting facilities. The risk under consideration is the likelihood of a malicious actor tampering with the equipment, software, or physical ballots used to cast and record votes so that vote tallies do not correspond with the voters’ selections.

Compromise Through Physical Access

An investigative report conducted by Reuters identified five instances in which staff of various U.S. counties illegally obtained or provided physical access to voting

¹ [hXXps://www.bbc\[.\]com/news/election-us-2020-54959962](https://www.bbc.com/news/election-us-2020-54959962)

²

[hXXps://www.axios\[.\]com/2022/09/30/stacey-abrams-lawsuit-2018-georgia-governors-election](https://www.axios.com/2022/09/30/stacey-abrams-lawsuit-2018-georgia-governors-election)

³

[hXXps://www.cisa\[.\]gov/uscert/ncas/current-activity/2022/10/05/fbi-and-cisa-publish-psa-malicious-cyber-activity-against-election](https://www.cisa.gov/uscert/ncas/current-activity/2022/10/05/fbi-and-cisa-publish-psa-malicious-cyber-activity-against-election)



equipment after the 2020 presidential election. Acting on unfounded rumors of falsified vote counts, the suspects in these cases sought or claimed to be preserving evidence of tampering that might have contributed to the election loss of their favored candidate. While these incidents occurred after votes had been certified at the state level and do not appear to have involved attempts to modify vote counts, they demonstrate the potential for equipment to be compromised by actors with approved physical access.

In one of the five cases, a town clerk provided access to a vote tabulator to three men recruited by a woman impersonating a federal elections official. One of the three, a computer technician, reportedly opened the tabulator and unsuccessfully attempted to insert a flash drive into multiple ports in an effort to extract voting data. Although no data was compromised in this intrusion,⁴ the incident provides a blueprint for a scenario in which skilled actors enter a polling location or counting facility, falsely claim authority to inspect equipment, interfere with systems for casting or counting votes, and modify results.

At a minimum, onsite voting systems consist of a vote-casting mechanism and a ballot receptacle. Touchscreen voting mechanisms are programmed in advance with the candidate choices for a given precinct (the “ballot definition”) through some form of removable media—often a flash drive.⁵ Scanners for tallying ballots are sometimes deployed at voting sites as well, and current versions are also programmed through removable media.⁶ A malicious actor in possession of a flash drive could, in theory, obtain access to a touchscreen voting machine at a voting site under the guise of being an elections official or technician, and insert content capable of altering voters’ selections. An actor would face formidable obstacles in attempting to compromise more recent releases of touchscreen voting devices. The most recent release of the touchscreen ExpressVote system by ES&S, for example, incorporates signed encryption that prevents further interfacing with a device once an election administrator has entered a ballot definition.⁷

⁴ [hXXps://www.reuters\[.\]com/investigates/special-report/usa-election-breaches/](https://www.reuters.com/investigates/special-report/usa-election-breaches/)

⁵

[hXXps://trumpwhitehouse\[.\]archives.gov/sites/whitehouse.gov/files/docs/pacei-dr-andrew-appel-report.pdf](https://trumpwhitehouse[.]archives.gov/sites/whitehouse.gov/files/docs/pacei-dr-andrew-appel-report.pdf)

⁶

[hXXps://www.dos.pa\[.\]gov/VotingElections/Documents/Voting%20Systems/ClearBallot/ClearVote-20-Secretarys-certification.pdf](https://www.dos.pa[.]gov/VotingElections/Documents/Voting%20Systems/ClearBallot/ClearVote-20-Secretarys-certification.pdf)

⁷ [hXXps://www.essvote\[.\]com/products/expressvote/](https://www.essvote[.]com/products/expressvote/)



Ballot marking device (BDE) and scanner used for tabulating votes

Source:

https://www.mlive.com/news/kalamazoo/2017/11/new_modern_voting_machines_for.html

However, counties throughout the United States implement a wide range of voting technologies of varying sophistication. In a review conducted by Pennsylvania's Department of State of an approved voting system currently used in the state, it is unclear whether that system has provisions for enforcing secure access similar to those touted by ES&S for ExpressVote.^{8 9}

Anecdotal evidence further suggests that voting equipment may be delivered to a site in advance of an election day. Sites used as polling locations include schools, churches, and other facilities that presumably do not meet high security standards and, in many cases, may be easily breached. Such facilities provide a considerable window for in-person compromise by determined actors.

Sites that use curtains to conceal voters introduce an added source of insecurity, as the activities of such voters cannot be monitored while interacting with voting equipment. Moreover, regulations that forbid curtaining may be lightly enforced at the precinct level. In Georgia, where state policy requires that voters remain visible while casting votes,¹⁰ local media has reported at least one instance of a precinct providing curtaining despite the requirement.¹¹

⁸ <https://www.eac.gov/voting-equipment/system-certification-process>

⁹

<https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/ClearBallot/ClearVote-20-Secretarys-certification.pdf>

¹⁰ <https://rules.sos.ga.gov/gac/183-1-12>

¹¹

<https://www.11alive.com/article/news/politics/elections/voting-machine-curtain/85-836581fe-ebec-492c-a0f5-996e55d3a085>



Compromise Through Online Access

A review of twenty state election policies suggests widespread awareness that strong security practices preclude connecting voting equipment directly to the internet.^{12,13} Despite this understanding, an election day exception is made by some states for reporting purposes. Some voting machines are equipped with vote tabulators containing embedded or externally-connected modems capable of transmitting unofficial vote tallies over wireless networks to SSH File Transfer Protocol (SFTP) servers housed within non-networked firewalls. These servers then relay the tallies to a centralized election reporting module. When implemented properly, this expedited form of reporting (enabling counties to provide early, provisional results to the public) involves only time-limited networked connections between voting equipment and wireless networks, which are in turn connected to internet infrastructure. Critics argue that these brief windows of connectivity are sufficient for malicious actors to infiltrate voting equipment through the modems and make changes to the voting software that could compromise present or future voter selections.^{14 15}

In 2019, a group of researchers led by Kevin Skoglund, a member of a cybersecurity advisory group for the U.S. Election Assistance Commission,¹⁶ identified 35 cases in which both the reporting modules and the centralized election management systems (EMS) configured to these specialized firewalls maintained connections to the SFTP servers after elections had ended, exposing them to the internet for prolonged periods. EMSes often provide the software updates used to program voting machines prior to elections. Exposed in this way, an EMS could potentially be used to distribute malware through flash drives to voting machines. The election modules could be attacked as well and made to report incorrect results. According to Skoglund, county officials notified of these vulnerable connections were surprised—an indication that resources for monitoring sensitive election assets are limited in many cases.¹⁷

Major voting technology providers (ES&S, Dominion, and Hart Intercivic) do not describe procedures for providing updates and patches of their software in publicly-accessible documents. To the extent that voting software updates are

¹² [hXXps://www.sos.wa.gov/elections/election-security.aspx](https://www.sos.wa.gov/elections/election-security.aspx)

¹³ [hXXps://dos.myflorida.com/elections/voting-systems/about-voting-systems/](https://dos.myflorida.com/elections/voting-systems/about-voting-systems/)

¹⁴

[hXXps://www.nbcnews.com/politics/elections/online-vulnerable-experts-find-nearly-three-dozen-u-s-voting-n1112436](https://www.nbcnews.com/politics/elections/online-vulnerable-experts-find-nearly-three-dozen-u-s-voting-n1112436)

¹⁵

[hXXps://freedom-to-tinker.com/2018/02/22/are-voting-machine-modems-truly-divorced-from-the-internet/](https://freedom-to-tinker.com/2018/02/22/are-voting-machine-modems-truly-divorced-from-the-internet/)

¹⁶ <https://csrcl.huji.ac.il/book/kevin-skoglund>

¹⁷

[hXXps://www.vice.com/en/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials](https://www.vice.com/en/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials)



distributed online to EMS hosts, the possibility of those updates being compromised in a manner similar to the SolarWinds attack of 2021 cannot be discounted.¹⁸

Analyst Commentary

Attacks against U.S. election equipment require a combination of skill and resources that is out of reach for most cybercriminals and hackers. Nation-states hostile to U.S. interests have demonstrated the capability to stage attacks that are broad in scale and highly sophisticated in execution. Given evidence indicating that U.S. election equipment is inconsistently secured, these assets present an attractive target to nation-state actors with an interest in causing discord resulting from election results being questioned.

Given the multiple vectors through which voting equipment can be compromised, votes recorded and tallied exclusively through electronic means cannot be verified with a high level of confidence. Only a system that includes some form of paper ballot can provide an adequate means of contesting or defending votes suspected of tampering. Such ballots can be optically scanned or hand-counted to verify election results.¹⁹ At present, some 67 percent of U.S. counties require voters to provide a hand-cast paper ballot in tandem with a digital vote. Most others provide either a physical ballot that is marked through a Ballot Marking Device (BMD) or a means of casting votes that is recorded electronically using Direct Recording Electronic Systems (DRE) in combination with a printed paper record (a Voter-Verified Paper Audit Trail or VVPAT). Because voters may not take note of digitally-marked or printed ballots that differ from selections made on compromised equipment, hand-cast ballots are more secure. At present, 5.1 percent of U.S. counties only provide non-verifiable DRE without VVPAT, suggesting a significant level of readiness to contest or defend a compromised election.²⁰

Recommendations

Election officials can ensure the highest level of security for the voting process by requiring voters to present a hand-cast, paper ballot in addition to any electronic casting of votes.

¹⁸

[hXXps://www.darkreading\[.\]com/edge-articles/3-years-later-solarwinds-ciso-shares-3-lessons-fr
om-the-infamous-attack](https://www.darkreading.com/edge-articles/3-years-later-solarwinds-ciso-shares-3-lessons-from-the-infamous-attack)

¹⁹ [hXXps://www.cs.princeton\[.\]edu/~appel/papers/bmd-insecure.pdf](https://www.cs.princeton.edu/~appel/papers/bmd-insecure.pdf)

²⁰

[hXXps://verifiedvoting\[.\]org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/20
22](https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2022)



Attempts to compromise election software can be countered by adopting a Zero Trust architecture on election systems, checking all requests for access to resources (such as software updates) against criteria provided by a wide range of sources before granting access. Wireless modems used for early reporting of election results are subject to intrusion and should not be implemented. Additionally, vulnerability scans should be conducted regularly on election systems to ensure there is no connectivity outside the LAN environments in which they are configured.



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.