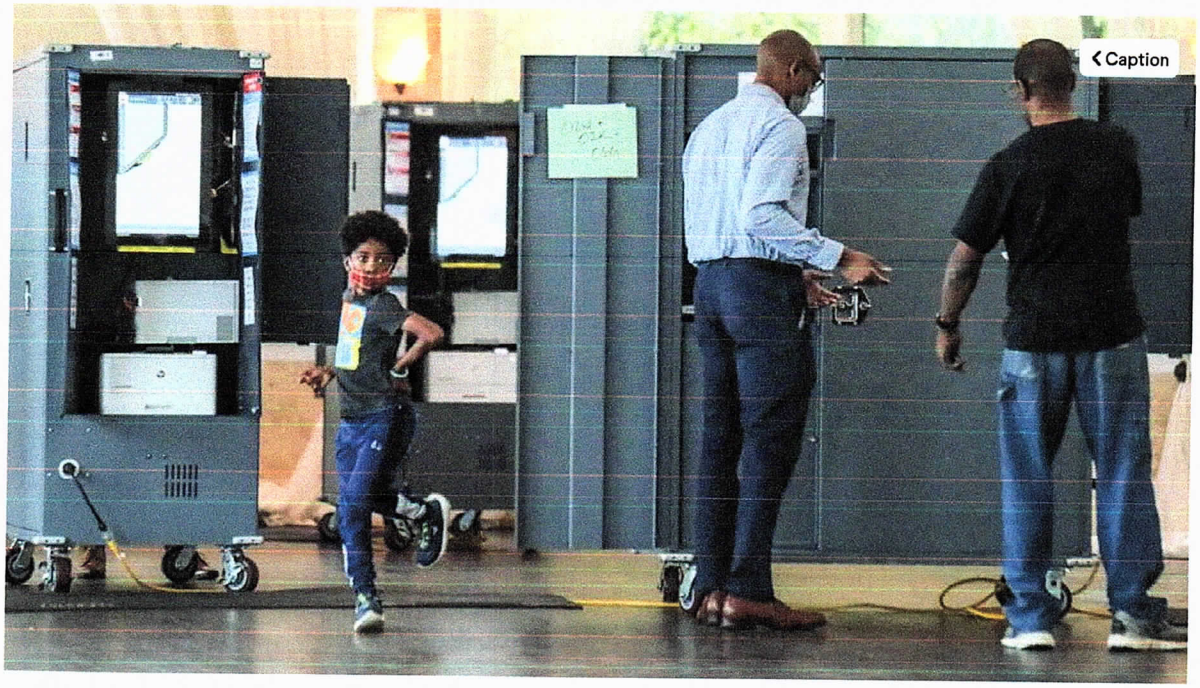
89°

The Atlanta Journal-Constitution

Georgia voting touchscreens vulnerable, cybersecurity agency finds



Credit: JOHN SPINK / AJC

POLITICS

By Mark Niesse, The Atlanta Journal-Constitution

June 3, 2022

Election officials say risk of tampering is remote

A U.S. cybersecurity agency reported Friday that voting touchscreens used in Georgia have security vulnerabilities that put them at risk to hacking attacks, though there's no evidence those weaknesses have been exploited so far.

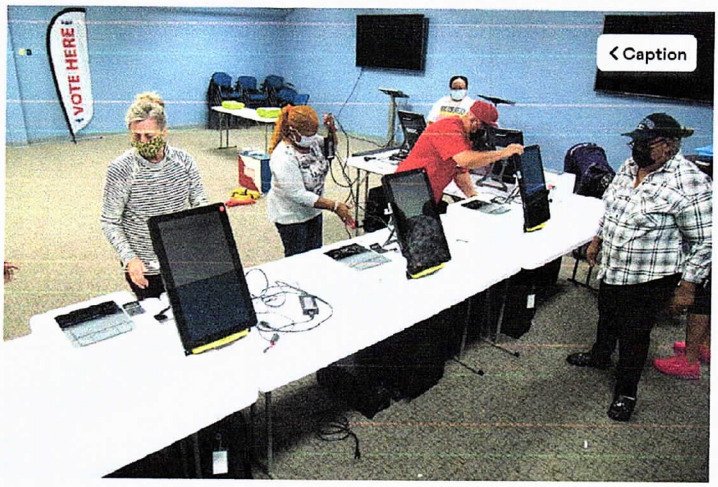
Election officials who rely on touchscreens manufactured by Dominion Voting Systems should increase security by conducting rigorous audits, strengthening physical protections of equipment and patching outdated software, according to recommendations by the U.S. Cybersecurity and Infrastructure Security Agency.

The report also says that state and county governments can choose to eliminate bar codes that are printed on ballots, which could be manipulated to change how votes are recorded. The Georgia secretary of state's office is considering abolishing bar codes.

The CISA report backs up allegations made in a federal court case that hackers could flip votes if they were able to gain access to voting equipment. After a four-month review, the agency cited nine vulnerabilities in Dominion's touchscreens.

Other companies' voting equipment could have similar flaws, but the CISA report focused on voting touchscreens used in Georgia. The review cited risks for future elections, and state investigations have repeatedly debunked allegations of fraud in the 2020 presidential election.

A Georgia election official said the real-world danger of hacking is remote because of layers of security in equipment that isn't connected to the internet.



Credit: Steve Schaefer

The secretary of state's office will review the recommendations, seek additional election audits and look for opportunities to improve election worker training, said Gabriel Sterling, chief operating officer for the secretary of state's office. Currently, state law only calls for one race to be audited every two years after general elections.

CISA Director Jen Easterly said the agency is working with election officials to address potential security deficiencies.

"Many of these mitigations, which are typically standard practice in jurisdictions where these devices are in use, are able to detect exploitation of these vulnerabilities and in many cases would prevent attempts entirely if diligently applied, making it very unlikely that a malicious actor could

exploit these vulnerabilities to affect an election," Easterly said.

Malicious code could be spread if someone gained physical access to voting touchscreens or the election management system computers that program them. In addition, hacks could infect voting equipment remotely if election workers used USB drives to transfer data from computers connected to the internet to election computers.

Georgia's statewide voting system uses touchscreens to print out paper ballots, which are then fed into scanning machines that record votes.

Because scanning machines read bar codes printed on the paper ballots, voters would have no way of knowing whether a hack had changed the bar code so that it didn't match the printed text of their choices.

Sterling said the flaws were only found after a federal judge allowed a computer scientist access to voting equipment and passwords.

"There's no way anybody can sit there in a real election environment and exploit any of these things," Sterling said. "Some of the vulnerabilities are there, but they're there in any system. We have lots of mitigation, and that's already built into our robust rules and laws."

The vulnerabilities were discovered by Alex Halderman, a computer science professor at the University of Michigan who is an expert for plaintiffs in a federal lawsuit seeking to replace Georgia's $138 million voting system with paper ballots filled out by hand.

Halderman's findings have been sealed in federal court since July, but CISA conducted its review to assess the threat to election security and provide advice to Georgia and jurisdictions in 16 other states that use the Dominion Democracy Suit ImageCast X voting equipment.

Election officials should pursue improvements to election technology, ballot security and post-election audits, Halderman said.

"The vulnerabilities are significant, and the state should take responsible steps promptly to reduce the risk that they'll be exploited," Halderman said. "That doesn't mean it's time to panic, and it doesn't mean that there is proof that any past election has been tampered with. But it does mean it's time to act."

Dominion said in a statement said the security of its voting system has been proven through thousands of elections and recounts.

"These issues require unfettered physical access to election equipment, which is already prohibited," a Dominion spokeswoman said.

A hack that exploited voting touchscreens could alter bar codes so that ballots were tabulated inconsistently with the human-readable text of the ballot, according to the CISA report. If that happened, voters won't be able to verify that their choices were what is actually counted.

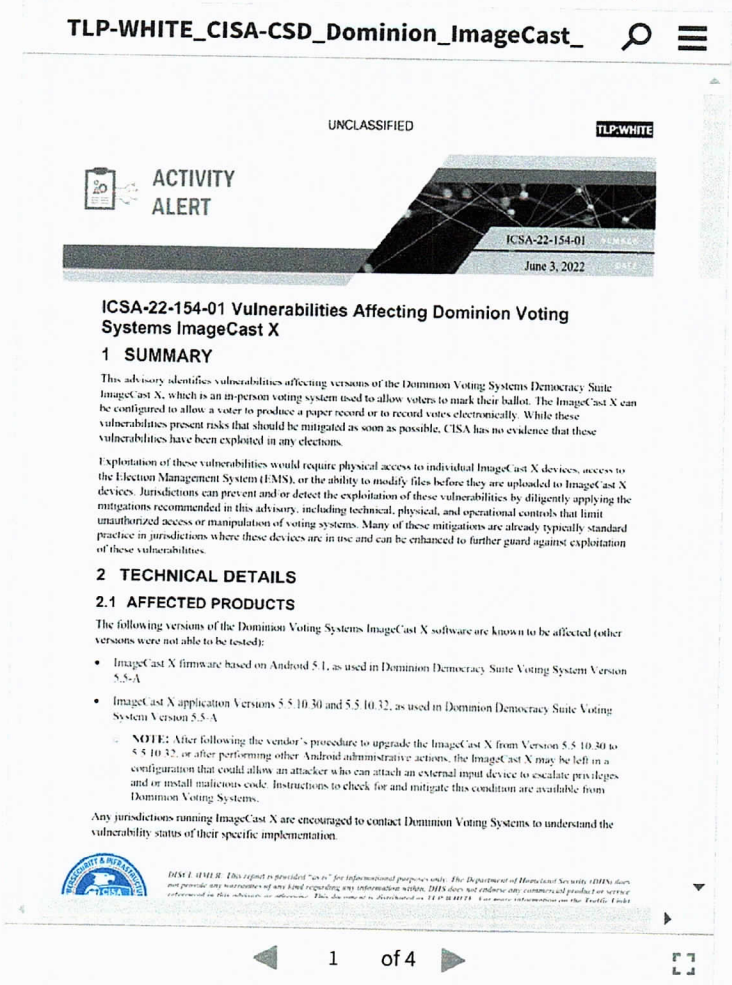
The secretary of state's office has been discussing whether to abandon bar codes in favor of a full ballot for more than a year, Sterling said. But that kind of change would create difficulties for auditing multipage ballots and drive up ballot printing costs borne by taxpayers.

Voters can help prevent the possibility of election tampering by reviewing printed ballots in polling places to ensure they're accurate, said Mark Lindeman, a director for Verified Voting, a national election integrity organization that focuses on election technology.

"Voters need to be able to check their ballots," Lindeman said. "It helps if you can hold a ballot and read it."

A study commissioned by the secretary of state's office found just 49% of voters spent at least one second looking at their printed-out paper ballots.

The CISA advisory also suggests that election officials encourage voters to verify the human-readable portion of printed ballots.



About the Author

Mark Niesse

Mark Niesse covers voting rights and elections for The Atlanta Journal-Constitution. He also reports on the Georgia House of Representatives and government. He has been a reporter at the AJC since 2013 following a decade at The Associated Press in Atlanta, Honolulu and Montgomery, Ala.

Editors' Picks

In Dansby Swanson, the Braves have much more than a shortstop. Can they keep him?

8h ago

Inside City Hall: Firm that copied Coffee Co. election files also has a contract with...

7h ago

Fulton DA: Burglary crew used TV, social media to target celebrity victims

1h ago