# Cyber agency: Voting software vulnerable in some states

apnews.com/article/2022-midterm-elections-technology-georgia-election-2020-a746b253f3404dbf794349df498c9542

May 31, 2022


By KATE BRUMBACKJune 1, 2022 GMT

FILE - Voting machines fill the floor for early voting at State Farm Arena on Monday, Oct. 12, 2020, in Atlanta. In an advisory sent to state election officials, and obtained by The Associated Press in advance of its expected release on Friday, June 3, 2022, the nation's leading cybersecurity agency says that electronic voting machines from a leading vendor used in at least 16 states have software vulnerabilities. The U.S. Cybersecurity and Infrastructure Agency, or CISA, said there is no evidence the flaws in the Dominion Voting Systems' equipment have been exploited to alter election results. (AP Photo/Brynn Anderson, File)

FILE - Voting machines fill the floor for early voting at State Farm Arena on Monday, Oct. 12, 2020, in Atlanta. In an advisory sent to state election officials, and obtained by The Associated Press in advance of its expected release on Friday, June 3, 2022, the nation's leading cybersecurity agency says that electronic voting machines from a leading vendor used in at least 16 states have software vulnerabilities. The U.S. Cybersecurity and

Infrastructure Agency, or CISA, said there is no evidence the flaws in the Dominion Voting Systems' equipment have been exploited to alter election results. (AP Photo/Brynn Anderson, File)

ATLANTA (AP) — Electronic voting machines from a leading vendor used in at least 16 states have software vulnerabilities that leave them susceptible to hacking if unaddressed, the nation's leading cybersecurity agency says in an advisory sent to state election officials.

The U.S. Cybersecurity and Infrastructure Agency, or CISA, said there is no evidence the flaws in the Dominion Voting Systems' equipment have been exploited to alter election results. The advisory is based on testing by a prominent computer scientist and expert witness in a long-running lawsuit that is unrelated to false allegations of a stolen election pushed by former President Donald Trump after his 2020 election loss.

The advisory, obtained by The Associated Press in advance of its expected Friday release, details nine vulnerabilities and suggests protective measures to prevent or detect their exploitation. Amid a swirl of misinformation and disinformation about elections, CISA seems to be trying to walk a line between not alarming the public and stressing the need for election officials to take action.

CISA Executive Director Brandon Wales said in a statement that "states' standard election security procedures would detect exploitation of these vulnerabilities and in many cases would prevent attempts entirely." Yet the advisory seems to suggest states aren't doing enough. It urges prompt mitigation measures, including both continued and enhanced "defensive measures to reduce the risk of exploitation of these vulnerabilities." Those measures need to be applied ahead of every election, the advisory says, and it's clear that's not happening in all of the states that use the machines.

## Full coverage


- **Court upholds ban against Cowboys for Trump co-founder**
- **Man pleads guilty to Capitol attack months after shooting**
- **Messages: Officer often fed information to Proud Boys leader**
- **Man who used stun gun on cop in Jan. 6 riot pleads guilty**

University of Michigan computer scientist J. Alex Halderman, who wrote the report on which the advisory is based, has long argued that using digital technology to record votes is dangerous because computers are inherently vulnerable to hacking and thus require multiple safeguards that aren't uniformly followed. He and many other election security experts have insisted that using hand-marked paper ballots is the most secure method of voting and the only option that allows for meaningful post-election audits.

"These vulnerabilities, for the most part, are not ones that could be easily exploited by someone who walks in off the street, but they are things that we should worry could be exploited by sophisticated attackers, such as hostile nation states, or by election insiders, and they would carry very serious consequences," Halderman told the AP.

Concerns about possible meddling by election insiders were recently underscored with the indictment of Mesa County Clerk Tina Peters in Colorado, who has become a hero to election conspiracy theorists and is running to become her state's top election official. Data from the county's voting machines appeared on election conspiracy websites last summer shortly after Peters appeared at a symposium about the election organized by MyPillow CEO Mike Lindell. She was also recently barred from overseeing this year's election in her county.

One of the most serious vulnerabilities could allow malicious code to be spread from the election management system to machines throughout a jurisdiction, Halderman said. The vulnerability could be exploited by someone with physical access or by someone who is able to remotely infect other systems that are connected to the internet if election workers then use USB sticks to bring data from an infected system into the election management system.

Several other particularly worrisome vulnerabilities could allow an attacker to forge cards used in the machines by technicians, giving the attacker access to a machine that would allow the software to be changed, Halderman said.

"Attackers could then mark ballots inconsistently with voters' intent, alter recorded votes or even identify voters' secret ballots," Halderman said.

Halderman is an expert witness for the plaintiffs in a lawsuit originally filed in 2017 that targeted the outdated voting machines Georgia used at the time. The state bought the Dominion system in 2019, but the plaintiffs contend that the new system is also insecure. A 25,000-word report detailing Halderman's findings was filed under seal in federal court in Atlanta last July.

U.S. District Judge Amy Totenberg, who's overseeing the case, has expressed concern about releasing the report, worrying about the potential for hacking and the misuse of sensitive election system information. She agreed in February that the report could be shared with CISA, which promised to work with Halderman and Dominion to analyze potential vulnerabilities and then help jurisdictions that use the machines to test and apply any protections.

Halderman agrees that there's no evidence the vulnerabilities were exploited in the 2020 election. But that wasn't his mission, he said. He was looking for ways Dominion's Democracy Suite ImageCast X voting system could be compromised. The touchscreen voting machines can be configured as ballot-marking devices that produce a paper ballot or record votes electronically.

In a statement, Dominion defended the machines as "accurate and secure."

Dominion's systems have been unjustifiably maligned by people pushing the false narrative that the 2020 election was stolen from Trump. Incorrect and sometimes outrageous claims by high-profile Trump allies prompted the company to file defamation lawsuits. State and federal officials have repeatedly said there's no evidence of widespread fraud in the 2020 election — and no evidence that Dominion equipment was manipulated to alter results.

Halderman said it's an "unfortunate coincidence" that the first vulnerabilities in polling place equipment reported to CISA affect Dominion machines.

"There are systemic problems with the way election equipment is developed, tested and certified, and I think it's more likely than not that serious problems would be found in equipment from other vendors if they were subjected to the same kind of testing," Halderman said.

In Georgia, the machines print a paper ballot that includes a barcode — known as a QR code — and a human-readable summary list reflecting the voter's selections, and the votes are tallied by a scanner that reads the barcode.

"When barcodes are used to tabulate votes, they may be subject to attacks exploiting the listed vulnerabilities such that the barcode is inconsistent with the human-readable portion of the paper ballot," the advisory says. To reduce this risk, the advisory recommends, the machines should be configured, where possible, to produce "traditional, full-face ballots, rather than summary ballots with QR codes."

The affected machines are used by at least some voters in at least 16 states, and in most of those places they are used only for people who can't physically fill out a paper ballot by hand, according to a voting equipment tracker maintained by watchdog Verified Voting. But in some places, including all of Georgia, almost all in-person voting is on the affected machines.

Georgia Deputy Secretary of State Gabriel Sterling said the CISA advisory and a separate report commissioned by Dominion recognize that "existing procedural safeguards make it extremely unlikely" that a bad actor could exploit the vulnerabilities identified by Halderman. He called Halderman's claims "exaggerated."

Dominion has told CISA that the vulnerabilities have been addressed in subsequent software versions, and the advisory says election officials should contact the company to determine which updates are needed. Halderman tested machines used in Georgia, and he said it's not clear whether machines running other versions of the software share the same vulnerabilities.

Halderman said that as far as he knows, "no one but Dominion has had the opportunity to test their asserted fixes."

To prevent or detect the exploitation of these vulnerabilities, the advisory's recommendations include ensuring voting machines are secure and protected at all times; conducting rigorous pre- and post-election testing on the machines as well as post-election audits; and encouraging voters to verify the human-readable portion on printed ballots.

___

This story has been corrected to reflect that Tina Peters has been barred from overseeing this year's election in her county, not from running for secretary of state.