https://www.thedailybeast.com/judge-seals-report-on-voting-machine-vulnerability?ref=scroll

DAILY BEAST

NATIONAL SECURITY

Judge Seals Report on Voting Machine Vulnerability

'ATTORNEYS' EYES ONLY'

A judge in a Georgia election security lawsuit is working to tamp down voting machine conspiracy theories. But sealing a court file could stoke the controversy even more.

Jose Pagliery

Political Investigations Reporter

Shannon Vavra

National Security Reporter

Published Aug. 13, 2021 4:28AM ET

It's the kind of report that could be weaponized by those looking to cast doubt on U.S. election results: a cybersecurity analysis that found flaws

in Georgia's voting machines and warns about the potential for future attacks. But a federal judge has sealed the report, and her attempt to shield the public from bad faith efforts to undermine the 2020 election could instead fuel the conspiracy theory dumpster fires—and keep the voting machine maker from figuring out how to fix it.

The 25,000-word report, commissioned by election integrity groups, does not touch on the 2020 results at all. But the report—authored by a University of Michigan computer science professor who has testified numerous times on Capitol Hill about U.S. election security, J. Alex Halderman—claims that Georgia's ballot marking devices (BMDs) "suffer from specific, highly exploitable vulnerabilities that allow attackers to change votes despite the state's purported defenses," all by using malware.

In a public court document, Halderman urged that his report be shared with Georgia election officials and the voting machine manufacturer to "address the vulnerabilities it describes before attackers exploit them."

Halderman wrote his report after he was given 12 weeks of access to an unused Dominion ICX voting machine, according to court documents. Several sources who spoke on the condition of anonymity told The Daily Beast that the secret report makes two points: hacking these specific ballot marking devices is easier than previously believed, and Georgia does not have a process in place to catch it if it ever happens.

"Georgia voters face an extreme risk that [ballot marking device]-based attacks could manipulate their individual votes and alter election outcomes," Halderman wrote in a signed declaration on Aug. 2.

While Halderman's claims are unverified, don't address the 2020 election, and provide no evidence that anyone has taken advantage of the alleged vulnerabilities, their mere existence will likely be enough for many "Stop the Steal" advocates who believe the 2020 results were illegitimate despite no evidence of widespread voter fraud.

Which is perhaps why U.S. District Court Judge Amy Totenberg made the report a "confidential document."

At a recent hearing, Totenberg sealed the report, citing a strong reluctance to draw any public scrutiny to the sensitive details in the case. Totenberg would not even allow an election integrity group to openly advocate for disclosure of the report, according to a transcript of a July 26 court hearing obtained by The Daily Beast. Instead, the judge asked that any such argument be filed in secret under seal.

"There are so many other ways to educate the public besides trying to use this case," Totenberg warned on the call. "I'm at the end of my rope about that."

The worry appears to be that this report could fuel baseless accusations by Trumpists, who are locked in court battles with Dominion. Federal judges in other states have tossed out multiple instances of the so-called "Kraken" lawsuits, alleging Dominion conspired with foreign countries to rig the election. Meanwhile, Dominion has filed defamation lawsuits against Fox News, Newsmax, One America News Network, and the former chief executive of Overstock.com.

Totenberg decided to limit circulation of the report, opting to keep it to "attorneys' eyes only"—and away from engineers at Dominion itself—

out of a concern that exposing it to company employees would make it "subject to disclosure in other litigation."

"I'm concerned enough about the information contained in it... I have seen how this can blow up," Totenberg said, according to the transcript.

That decision could stoke conspiracy theorists, but experts in the right-wing media ecosystem were also concerned that any information about potential issues with voting machines might be exploited.

Sam Jackson, an assistant professor who teaches about online extremism at the University at Albany, told The Daily Beast that the mere existence of this story could fuel conspiracy theories.

"I would not be surprised to see some far-right media outlets run very inflammatory headlines that are deliberate misreadings of this piece," he said.

Matt Gertz, a senior fellow at Media Matters for America, which scrutinizes right-leaning media, expects the "very well-developed conspiracy theory network" built in recent years on social media and alternative TV stations like Newsmax and One America News Network to wrongfully use the existence of the report to "undermine the validity of elections in the minds of conservatives."

"They will use anything they can to fan the flames of these conspiracy theories," Gertz said.

But those efforts to poke holes in the 2020 election haven't played out quite yet. Just this week, the lead information technology consultant for MyPillow CEO Mike Lindell—who has alleged in a much-touted

conspiracy theory that China hacked the 2020 election—admitted they don't actually have any proof of election fraud, debunking their own claims.

The important distinction others might miss in the Georgia case is that the cybersecurity analysis discovered vulnerabilities that *could* be used, not evidence that an actual hack ever occurred.

In order to successfully launch the malware, attackers would need a number of things to go their way. They'd have to gain "temporary physical access" to individual Dominion ICX machines, or infect them before they are placed at polling locations by tapping into them while they're being programmed "remotely from election management systems," Halderman said in court filings.

The document detailing the vulnerabilities remains sealed, so the specific workings of the flaws—and how easy it would be for a would-be attacker to take advantage—are not clear. Halderman notes in a court filing that the Dominion ICX devices in question "can be hacked, including by a voter in a voting booth in mere minutes."

Although The Daily Beast was briefed on the report by two people who had read it, The Daily Beast has not obtained the report and cannot independently verify Halderman's claims. Halderman declined an interview for this story.

As laid out in court documents, one of Halderman's main concerns is that the Dominion ICX machines used in Georgia print out QR codes meant to represent the voters' intended choice—but the voters can't read the QR codes to verify that their votes have been recorded as they

intended. This is already a problem for voters interested in verifying their votes are accurately recorded.

Halderman's hypothetical attack would not touch the person's choices at the outset, but secretly alter the QR code that actually is used to record the vote, further muddying the waters, according to court filings.

Halderman notes that the election integrity activists' lawyers who hired him to conduct the study have repeatedly tried to broker a meeting between him and Dominion to confidentially share details about the flaws, which could prevent any accidental disclosures through discovery.

"However, Dominion has yet to agree to meet," Halderman writes in his July 12 signed declaration. "It would be dangerous to provide Dominion with the complete report if it were then disclosed through discovery in the company's various ongoing defamation suits to anyone who might misuse it."

A Dominion spokesperson told The Daily Beast it generally welcomes feedback, declining to answer questions about Halderman's requests and whether it wants to know the specific details of the report.

"Despite continued defamatory attacks against our company and its systems, Dominion has emerged from the 2020 election cycle with arguably the most tested, most scrutinized, and most proven voting technology in recent history. Our company welcomes feedback that is provided in good faith by researchers," the spokesperson said. "We don't have further comment at this time related to the ongoing litigation in question."

Halderman has also offered to submit a redacted or modified version of this report so that hackers can't take advantage, arguing in that July 12 filing that disclosing flaws helps law enforcement spot future attacks, guides local election officials who are buying new voting machines, and gives manufacturers time to fix similar problems.

He noted that past cybersecurity reviews in California and Ohio in 2007 struck the right balance, making just enough information public to address flaws without providing hackers a blueprint.

While the document remains sealed, the flaws can't be fixed—an oversight that ought to be remedied swiftly, security experts tell The Daily Beast.

Even so, Matt Bernhard, an election security advocate, cautioned that the existence of the flaws isn't all that earth-shattering, given the often-uneven track record of voting technology vendors with security; researchers have been finding flaws in various companies' voting machines for years.

"It's pretty obvious that there are going to be flaws in their system," said Bernhard, a research engineer at VotingWorks, adding that all kinds of voting technology from a multitude of vendors have flaws. "I have no doubt in my mind that Dominion has serious flaws in their voting system," he said. "It's not shocking."

Election security expert Eddie Perez, the global director of technology development and open standards at the Open Source Election Technology Institute said he wasn't sure the technical findings are that

outlandish. But based on the court filings he has seen, he said it sounded like the vendor needed to take a look.

"Having read a lot of technical reports, I want to be clear: I don't know if I would classify this as a bombshell or not," Perez said. "But it is certainly a concern."

Still, Perez argued it was "within the public interest" to expose these vulnerabilities. "This demands action from the appropriate authorities," he said.

Richard DeMillo, an election security expert and former chief technology officer at Hewlett-Packard, told The Daily Beast he is concerned that keeping the report under lock and key may unnecessarily raise suspicions among conspiracy theorists and warned that "legitimate scientific results will be misquoted."

"The 'Stop the Steal' people don't need much excuse to have their conspiracy theories fanned," DeMillo said. "So keeping [it] secret probably plays into their hand, too. They can say, 'They know secrets and they're not telling us and that's cause for not trusting the whole system.'"

In the meantime, the solution is incredibly simple, Halderman says: switch to hand-marked paper ballot systems, in which experts say technology can't alter the choices voters mark down.

"Georgia can eliminate or greatly mitigate these risks by adopting the same approach to voting that is practiced in most of the country: using hand-marked paper ballots and reserving BMDs for voters who need or

request them," Halderman writes in a court filing. In this case, "these vulnerabilities would have little potential to change election outcomes."

Georgia's Secretary of State's office did not return repeated requests for comment.

However, the agency's chief operating officer, Gabriel Sterling, told a group of attendees at a professional luncheon in Sandy Springs, Georgia on Tuesday that he thinks "Halderman's report is a load of crap," according to an audio recording that was leaked to The Daily Beast.

Sterling and the Secretary of State's office did not return a request for comment to elaborate on his understanding of the report.

There is now growing concern that distrusted entities conducting partisan reviews of the 2020 election—like the so-called Cyber Ninjas in Arizona (whose effort has been riddled with security errors and mismanagement from the get-go) and MyPillow's Lindell elsewhere—have gained access to Dominion software and could discover these flaws as well.

It's unclear whether any of these groups have acquired the software that runs on ICX machines, but Lindell supporters who joined him for a conspiracy-fueled lovefest this week in South Dakota revealed they copied the contents of a Dominion computer server, according to reports from the conference.

The worry about these people gaining privileged access is heightened because conspiracy theorists may be incentivized to cheat in future elections, egged on by former President Trump, who continues to falsely

accuse Democrats of cheating in the previous election. As Trump said last month during a conspiracy-laden speech in Phoenix: "When they steal it from you and rig it, that's not easy. We have to fight. We have no choice."

It's a particular concern for Philip Stark, a statistician at University of California Berkeley who created a well-known type of election audit and is one of the few who has seen the secret report.

"Given that they've had unfettered access and in principle could discover the same vulnerabilities, any pretext of security through obscurity ought to be considered lost," he told The Daily Beast.

"If a single professor in Ann Arbor, Michigan over the course of a couple of months can figure it out," DeMillo added, "certainly [others] can figure it out, too."