ZeroHedge | On a long enough timeline the survival rate for everyone drops to zero.

Dominion Voting Machines In 16 States Vulnerable To Hacks: Cyber Agency

BY TYLER DURDEN

THURSDAY, JUN 02, 2022 - 03:25 AM

Dominion Voting Systems machines used in at least 16 states have software weaknesses that make them vulnerable to hacking, the U.S. Cybersecurity and Infrastructure Agency (CISA) has warned election officials.

According to AP, which obtained the CISA advisory ahead of an anticipated Friday release, the agency said it has no evidence these vulnerabilities have actually been exploited, but is urging states to implement measures to prevent and detect hacking.

> **"One of the most serious vulnerabilities could allow malicious code to be spread from the election management system to machines throughout a jurisdiction**...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," AP reports.

The 16 states weren't identified. According to the company's website, **Dominion products are used in 28 states and nine of the 20 largest counties in the country.**

The CISA advisory was prompted by a 25,000-word report by J. Alex Halderman, a University of Michigan computer scientist. He prepared the report as an expert witness in a federal lawsuit filed by

voting integrity activists who want Georgia's machines replaced with paper ballots. The suit was filed in 2017 and is unrelated to any allegation of a specific hack.

Election-hackers could exploit other weaknesses to forge cards technicians use to access—and change—the machines' software. **“Attackers could then mark ballots inconsistently with voters’ intent, alter recorded votes or even identify voters’ secret ballots,”** Halderman told AP.

State and federal election officials maintain they have no evidence that Dominion equipment was tampered with to change 2020 election tallies. Dominion is suing Fox News, Rudy Giuliani and others for defamation, over their suggestions the company's voting machines enabled fraud in that election.

CISA is recommending that, in jurisdictions where the Dominion voting machines are used, officials should implement safeguards such as testing of machines before and after elections, post-election audits, and asking voters to confirm the readable portion of machine-generated paper ballots.

However, even according to the CISA advisory, voter confirmation of the human-readable, computer-generated paper ballot can be skirted by hackers. Automated counting of ballots is done by reading a QR code printed on them, and CISA warned that some of the software vulnerabilities could allow hackers to generate a code that's "inconsistent with the human-readable portion of the paper ballot.”

Halderman's report is being kept under seal; U.S. District Judge Amy Totenberg says she's wary the report, if made public, would serve as a user's manual for bad actors. **Halderman's report has been designated "attorneys' eyes only,"** which means even the parties to the suit aren't allowed to read it.

Dominion is at the center of the CISA advisory because the Georgia lawsuit that prompted Halderman's report centers on Dominion machines, which are used for nearly all in-person voting in the state.

> **"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,”** said Halderman.

Halderman and his students have successfully hacked voting machines in their own tests. In 2017 testimony for the Senate intelligence committee, Halderman, speaking about voting machines in general, said:

> “**We’ve created attacks that can spread from machine to machine like a computer virus and silently change election outcomes. We studied touch screens and optical scan systems. And in every single case, we found ways for attackers to sabotage machines and to steal votes.**”

Halderman recommended universal adoption of optical scan ballots, where voters manually fill in paper ballots that are scanned and counted by a computer—along with the inspection of a sufficient quantity of paper ballots to verify that optical scanners are compiling an accurate tally.

"Paper provides a resilient physical record of the vote that simply can’t be compromised by a cyberattack," he said.

PRIVACY POLICY

DISCLAIMER

ADVERTISE WITH ZEROHEDGE