New American

Written by **Rebecca Terrell** on June 4, 2022

U.S. Voting Machines Vulnerable After All

The nation's top cybersecurity agency admits software vulnerabilities in electronic voting machines used in many states.

AP Images

In an advisory publicly released on Friday, the U.S. Cybersecurity and Infrastructure Agency (CISA) identified nine flaws in Dominion Voting Systems software. Dubbed the Democracy Suite ImageCast X, it is an interactive technology that allows voters to mark their ballots electronically.

The advisory says that Dominion machines are susceptible to manipulation by those with physical access to the voting devices or access to the Election Management System (EMS). The latter is software called Democracy Suite, which the company says powers "all Dominion products."

CISA's advisory also warns that Dominion technology is open to hackers who could modify files even "before they are uploaded to ImageCast X devices."

The agency assures state election officials that they can "prevent and/or detect" such attacks if they "diligently" apply controls recommended by CISA. Despite that strong warning, the advisory bulletin disarmingly declares that many of the agency's recommendations "are already typically standard practice … and can be enhanced to further guard against exploitation" by would-be hackers.

CISA is the same agency that issued a November 13, 2020 statement calling that year's general election just 10 days prior, "the most secure in American history."

Regardless, should newly admitted chinks in the armor of voting software raise concern about past elections? The agency says not. "While these vulnerabilities present risks that should be mitigated as soon as possible," reads their June 3 press release, "CISA has no evidence that these vulnerabilities have been exploited in any elections."

The Associated Press (AP) underscored that point in typical mainstream Trump-bashing style. Having obtained a leaked copy of the CISA advisory, which was distributed to election officials one week prior to public release, the news outlet reported on May 31 that the announcement is "unrelated to false allegations of a stolen election pushed by former President Donald Trump after his 2020 election loss."

Such protestations notwithstanding, Dominion and its chief competitors, Hart InterCivic and Election Systems & Software (ES&S), were under fire long before 2020.

In 2019 *Politico* reported that glitches in ES&S technology potentially skewed races in the previous year's elections in Georgia. The article recalled lawsuits in 2017 filed by "election-integrity groups that say the machines are not secure and want the state to switch to paper ballots that can be audited."

Also in 2019, ProPublica revealed similar cases in Indiana and Florida. Additionally, Texas refused to

certify Dominion's voting technology that year, while "the state also saw hundreds of aging Hart machines confusing voters and leading to accusations of vote flipping."

The problems caused by ES&S in Georgia's 2018 elections prompted state officials to replace them with Dominion products. Yet two months prior to the 2020 election, AP reported that the "new system has many of the same security vulnerabilities as the old system."

Investigations since then have identified "multiple severe security flaws" in the voting devices, as noted by election security expert J. Alex Halderman of the University of Michigan, in a 2021 sworn court declaration.

CISA's latest advisory names Halderman as one of two researchers who "reported these vulnerabilities" to the agency. His co-investigator was Drew Springall of Auburn University.

The security flaws that Halderman and Springall identified include multiple software vulnerabilities that allow attackers to upload and disguise malicious code or applications directly on Dominion devices or through the EMS. Other weaknesses allow hackers to gain elevated privileges or perform administrative actions. There is even a flaw in the voter interface process that allows the user to print "an arbitrary number of ballots without authorization."

Election integrity expert Patrick Colbeck, former vice chair of Elections and Government Reform in the Michigan Senate, questions CISA's assertion that there is no evidence that any of these weaknesses were ever misused. "Perhaps the specific vulnerabilities identified in their advisory may not have been exploited," he writes at his website LetsFixStuff.org, "but it is disingenuous to give the impression that there is no evidence of electronic voting system exploits." He provides three examples of Dominion voting machine anomalies in Tennessee, Georgia, and Colorado.

Colbeck also notes the interesting timing of CISA's announcement. "While media stories about the security vulnerabilities of electronic voting systems were all the rage in the lead up to the 2020 election, such narratives were actively suppressed" afterward, he opines. "That's what makes the sudden interest in stories about security vulnerabilities in the lead up to the 2022 election so interesting."