CYBERSECURITY

# The nation's best hackers found vulnerabilities in voting machines — but no time to fix them

Organizers and participants at the DEF CON Voting Village found cyber vulnerabilities in everything from voting machines to e-poll books, but there is no time before the November elections to fully implement their findings.


Election Day security is under particular scrutiny in 2024. | Elijah Nouvelage/Getty Images

By **MAGGIE MILLER**
08/12/2024 04:00 PM EDT

LAS VEGAS — Some of the best hackers in the world gathered in Las Vegas over the weekend to try to break into voting machines that will be used in this year's election — all with an eye to helping officials identify and fix vulnerabilities.

The problem? Their findings will likely come too late to make any fixes before Nov. 5.

In one sense, it's the normal course of events: Every August, hackers at the DEF CON conference find security gaps in voting equipment, and every year the long and complex process of fixing them means nothing is implemented until the next electoral cycle.

But Election Day security is under particular scrutiny in 2024. That's both because of increasing worries that foreign adversaries will figure out how to breach machines, and because President Donald Trump's unsubstantiated

allegations of widespread fraud in 2020 undermined confidence in the vote among his supporters.

As a result, many in the election security community are bemoaning the fact that no system has been developed to roll out fixes faster and worrying that the security gaps that get identified this year will provide fodder for those who may want to question the results.

“As far as time goes, it is hard to make any real, major, systemic changes, but especially 90 days out from the election,” said Catherine Terranova, one of the organizers of the DEF CON “Voting Village” hacking event. She argued that’s particularly troubling during “an election year like this.”

From Friday to Sunday, Voting Village hackers clustered around tables with all shapes and sizes of voting machines and equipment to verify voters’ identities or tabulate ballots, trying to get past firewalls or other security measures. Nearby, secretaries of state and other election officials gave talks on misinformation and disinformation threats facing the upcoming election.

Unlike most of the other events at the conference though, the Voting Village was not on the main show floor. It was a decision organizers said was necessary in order to ensure security following years of hatred flung at the event online by those who see the hackers as undermining democracy. In recent years, individuals associated with election denialism showed up at the Voting Village to harass organizers and speakers.

The findings, at times ignored or resisted by the manufacturers of voting machines, have increasingly been accepted in Washington, and the event is often seen as key for boosting the security of machines.

And just like every year since the Voting Village began almost a decade ago, attendees found problems. Organizers of the Voting Village intend to put out a full report in the coming weeks detailing the vulnerability findings from this cycle, and according to Voting Village co-founder Harri Hursti, these vulnerabilities ran “multiple pages” as of Saturday afternoon. While Hursti would not comment on the exact problems found, the amount was fairly consistent with previous years.

Those discoveries come amid ongoing foreign and criminal targeting of U.S. elections. In 2016, Russian hackers both targeted the campaign of Democratic presidential candidate Hillary Clinton and compromised voter registration databases in multiple U.S. states. It’s affecting this election cycle already, as POLITICO first reported Saturday that the presidential campaign of former President Donald Trump was hacked, a breach the campaign attributed to Iran.

While there’ve been no foreign cyberattacks taking wide swaths of voting machines offline on election day or evidence of hacks that affected results, the risk is always there.

“If you don’t think this kind of place is running 24/7 in China, Russia, you’re kidding yourselves,” Hursti said, gesturing around the room of voting equipment. “We are here only for two and a half days, and we find stuff…it would be stupid to assume that the adversaries don’t have absolute access to everything.”

Any issues found in these machines — most of which are used in at least one jurisdiction around the U.S. — would need to go through a complex process to be fixed, and that takes much longer than the two months until the November general election.

Voting Village organizers are frustrated that, despite years of security findings, voting machines vendors aren't moving more quickly to make fixes.

"There's so much basic stuff that should be happening and is not happening, so yes I'm worried about things not being fixed, but they haven't been fixed for a long time, and I'm also angry about it," Hursti said during a break in the day.

While there is a robust system in place for certifying voting systems, it's a long

"Even if you find a vulnerability next week in a piece of modern equipment that's deployed in the field, there's a challenge in getting the patch and getting the fix out to the state and local elections officials and onto the equipment before the November election," said Scott Algeier, executive director of the Information Technology-Information Sharing and Analysis Center. The group serves as a way for companies in the IT space to share threat information.

Algeier, who also runs the organization's Elections Industry Special Interest Group, said the process involves getting sign off from the machine manufacturer, then getting the system recertified by relevant authorities, then going in and updating each device. This complex series of steps is complicated even more by most election machines behind locked down weeks in advance of the elections.

"It's not a 90-day fix, It's not a Microsoft every Tuesday, issue your patch and everything works fine," Algeier said. "It's a pretty complicated process."

There are some proposals to speed up the process so election officials aren't scrambling to update voting machines every time DEF CON happens in an election year. For example, some argue that depending too much on one annual event at a private conference is not the best approach.

One option to speed up the process? Bring voting machine vendors together with hackers in a more formalized setting. The Elections Industry-SIG hosted an event last year in Washington that did just that, and helped to build bridges between a typically suspicious industry and security researchers.

"We want to build a program where we can work in partnership with the security researchers, under the principles of coordinated vulnerability disclosure," Algeier said.

Until then, for those who packed the Voting Village this weekend, with lines spilling out in the hallway, the event serves a higher purpose.

"We may not be able to fix everything about our election system in the next 90 days, but we can start by getting some of our facts straight and by understanding how our election systems work," Terranova said.

**FILED UNDER:** CYBER SECURITY, LAS VEGAS, DONALD TRUMP, DONALD TRUMP 2024,

# Playbook

The unofficial guide to official Washington, every morning and weekday afternoons.

EMAIL

Your Email

EMPLOYER

Employer

JOB TITLE

Job Title

By signing up, you acknowledge and agree to our Privacy Policy and Terms of Service. You may unsubscribe at any time by following the directions at the bottom of the email or by contacting us here. This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

SIGN UP