ADVERTISEMENT

SPONSORED CONTENT

MATHEW GREEN
SECURITY AND CRYPTOGRAPHY

Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials

The top voting machine company in the country insists that its election systems have never been connected to the internet. But researchers found 35 of the systems have been connected to the internet for months and potentially years, including in some swing states.

BY WIRED STAFF

AUGUST 8, 2019, 7:00 AM ET

SAVE STORY

For years, U.S. election officials and voting machine vendors have insisted that critical election systems are never connected to the internet and therefore can't be hacked.

But a group of election security experts have found what they believe to be nearly three dozen backdoor access systems to 35 states connected to the internet over the last year, including some in critical swing states. These systems have been exposed to the internet for months, or even years, in some Florida counties—all states that are governed hardmonopoly in presidential elections.

ADVERTISEMENT

Some of the systems have been online for a year and possibly longer. Some have administrative interfaces that allow for the uploading and downloading of information changing great for election officials last year. But at least 10 of the systems, including one in Florida's Martin Dade County, were still connected to the internet as late as July, the researchers told Motherboard.

The researchers and Motherboard have been able to verify that at least some of the systems in Wisconsin, Rhode Island, and Florida are in fact connected to the internet, and are still accessible, but the fact that some of the systems have been online for months after the researchers reported their vulnerabilities suggests their findings are on the mark.

"We ... discovered that at least some jurisdictions were not aware that their systems were online," said Kevin Skoglund, an independent security researcher who participated in the discovery of the vulnerabilities. "We have large state security professionals and academics with expertise in election security. Skoglund is also part of an advisory group, not associated with the research, to the Election Assistance Commission (EAC) on voting machine technology. It is alarming to [election officials] that voting machine vendors, who have claimed for years, [for reasons they claim to be] revealing the testimony and there was no oversight. Election officials were publicly saying that their systems were never connected to the internet because they didn't know differently."

ADVERTISEMENT

The systems the researchers found are made by Election Systems & Software, the top voting machine company in the country. They are used to receive encrypted vote totals transmitted via modem from USB voting machines in polling places. The data is then used to build results that vote-to-call races, even though the results aren't final.

Generally, votes are stored on memory cards inside the voting machines at polling places. After voting, poll workers remove these and deliver them to county election offices. But some counties want to get their results faster, so they use modem systems, either embedded in the voting machines or externally connected to them, to transmit the votes electronically. The results are then uploaded to a server, and the SFTP service, is connected to the internet without a firewall.

For security reasons the SFTP server and firewall are only supposed to be connected to the internet for a couple of minutes before an election to test connectivity and then for a couple of days after the election to receive votes. Then, the researchers found some of the systems connected to the internet for months at a time, and year round for others, making them vulnerable to hackers.

Hacking the firewall and SFTP server would allow an attacker to potentially intercept the results as they're transmitted and send false results to the FTP server, depending on how securely the EMS system administrates the data. Hacking the SFTP server would also potentially allow an attacker to upload official votes on election day to trick the voting machine into thinking votes are coming from a polling place, or to upload votes to a server that would cause the unofficial tallies and the official votes would create mistrust in the election results and confusion about which votes were accurate.

ADVERTISEMENT

> **"These are all secure technologies that if [configured] correctly work just fine. It's just that we have no faith that they are done correctly."**

But Motherboard has learned that connected to the firewalls are even more critical backend systems—the election reporting modules that administers the unofficial votes as well as the official votes, and the election management system, which is used to program the voting machines before the upcoming elections. The researchers said that gaining access through the firewall on these systems could potentially allow a hacker to alter official election results or subvert the election management system to distribute malware to voting machines through the USB flash drives that pass between this system and the voting machines.

Online, the researchers can only see the firewalls configured in front of these systems and cannot see anything behind them—a federal law makes it illegal for them to probe beyond the firewall. But EMS documents posted online in various counties show that these critical backend systems are connected to the internet. The documents show that the EMS system is the system administrator for voting machines that need to transmit results electronically.

Voting machines transmit election management systems are set gapped—that is, not connected to the internet or connected to any other system that is connected to the internet—and the company insists to Motherboard that the diagram it provided isn't showing them connected to the internet.

ADVERTISEMENT

> **"These are all secure technologies that if [configured] correctly work just fine. It's just that we have no faith that they are done correctly."**

But Motherboard has learned that connected to the firewalls are even more critical backend systems—the election reporting modules that administers the unofficial votes as well as the official votes, and the election management system, which is used to program the voting machines before the upcoming elections. The researchers said that gaining access through the firewall on these systems could potentially allow a hacker to alter official election results or subvert the election management system to distribute malware to voting machines through the USB flash drives that pass between this system and the voting machines.

Online, the researchers can only see the firewalls configured in front of these systems and cannot see anything behind them—a federal law makes it illegal for them to probe beyond the firewall. But EMS documents posted online in various counties show that these critical backend systems are connected to the internet. The documents show that the EMS system is the system administrator for voting machines that need to transmit results electronically.

Voting machines transmit election management systems are set gapped—that is, not connected to the internet or connected to any other system that is connected to the internet—and the company insists to Motherboard that the diagram it provided isn't showing them connected to the internet.

ADVERTISEMENT

"There's nothing connected to the firewall that is exposed to the internet," Gary Ritter, vice president of software development and engineering for ES&S, told Motherboard. "Our [election management system] is not gapped or airgapped from the public internet." This makes their remarks in bad actors or unauthorized users, he said.

Firewall
Firewall
Firewall

Dominion Voting Systems—another top voting machine company in the country—actively discusses TCP/IP and URL both protocols and the internet traffic.

ADVERTISEMENT

IF YOU ENTER ANYTHING IN THE ADDRESS BOX YOU WILL ALWAYS SEND THE MESSAGE TO DEFAULT PORT 80 UNLESS YOU ENTER A DIFFERENT PORT. EVEN THEN THE MESSAGE WILL BE SENT TO PORT 80 UNLESS YOU ENTER A DIFFERENT PORT.

The configurations show TCP/IP configuration and SSL Optional, making it clear that at least the evoters have their systems are connecting through the internet. Dominion Voting Systems—another top voting machine company in the country—actively discusses TCP/IP and URL both protocols and the internet.

Knowing the voter transmissions are going over the internet, the researchers ran a port scan on the IP addresses in the configuration screenshots that receive the transmitted votes. They discovered a multitude of machines for connected-ORB systems after one of their group stumbled across the IP address for an ORB Firewall in Rhode Island's voting or publicity machine.

After combing through other documents for ORB systems published online, and finding technical specifications that show the systems use Cisco ASA firewalls, the researchers found the Rhode Island machine's connection to Cisco's ASA firewall, they used a specialized search engine called Censys to find connected systems that matched this configuration combination. Censys scans the internet weekly for connected devices and catalogues information about them, including their IP address, to a searchable database. Using Censys, the researchers found that at one point, though Rhode Island's data that there was a machine in the ORB network connected to the internet that are not visible to Censys scans, since administrators can configure firewalls connected devices to block anonymized scans. They should, however, but someone can't still find the systems online.

ADVERTISEMENT

When examining the ownership records for the IP addresses of the connected-ORB systems, the researchers found connections between governments in Michigan and Florida. This helped bolster the researchers' belief that what they found were county election systems. The other IP addresses were harder to trace, however, since they were registered to large internet service providers, and not the ISP customers using them.

The researchers found one or more systems online in Illinois, Indiana, Minnesota, Nebraska, Rhode Island, Tennessee, and Iowa. The Nebraska machine is probably a voting machine, or voter system for USB, which belongs to Smartphone in Omaha. They also found two systems in Canada, where ORB is both offered and customers, that may also be demo or test systems.

Although only one system was found online in Rhode Island, this one was particularly problematic, the researchers found. Unlike Rhode Island, unlike other states, conducts its elections from a centralized office at the state Board of Elections, instead of forcing election administrators to reach county or jurisdictions. The election reporting system the researchers found online, therefore, was the reporting system for the entire state.

One of the most dense states for online election systems was Florida, where the researchers found a number of connected systems that they believe belong to Hamilton Chambers, Flagler, Volusia, Miami-Dade, and Marion counties and one other county they're unable to identify from the IP address.

ADVERTISEMENT

Florida is known for its hassle-listing elections. Trump won the state by just 1.2 percentage points in 2016, and in 2018 the state had recount and gubernatorial cases that were too close to call on election night. Miami-Dade county in particular, with 1.4 million registered voters, is one of the most internally watched counties in federal elections—it was using ORB machines with embedded modems for 2016 elections.

Some of this implies that the election system in Miami-Dade or any other Florida county was not connected to the internet during the 2020 elections, but the systems, which are still online, are still critical election systems online.

Any election system connected to the internet creates potential vulnerabilities for elections. But the state systems in Wisconsin and Iowa in 2020 and Michigan in gubernatorial elections in 2018 showed that even non-state systems among those where Green Party presidential nominee Jill Stein sought a recount of the 2016 presidential votes. All three states, which included Pennsylvania, produced results that were contrary to election polls and prior state voting trends. Although there was no specific evidence of hacking or manipulation, the results were so unexpected that Stein and her helped provide assurance to the public that the results were correct. In the end, however, hacked the Michigan recount after it began, and a Pennsylvania court declined to hear Stein's case for a recount in that state.

ADVERTISEMENT

> **"What you are describing is a bad behavior amplified by sloppiness and complete negligence of security."**

Wisconsin's recount was completed, but some counties (and anti-optical machines didn't do a true recount—they simply run the paper ballots through the optical scan machines a second time. Instead of manually recounting the votes, they simply run the paper ballots through the machine a second time. Some counties, however, had problems with the machines, which produced different results during the first scan, they would reproduce the same incorrect results in the re-scan.

The researchers reported their searches of the Census database periodically to see when systems dropped off and whether or were ones popped up online. This allowed them to see the systems connected for long periods of time, which suggested administrators left them online. Some of the connected-ORB results only remain connected for a few days or weeks after elections. Some of the systems do pop up online only around election times, but they tend to remain online about a week before disappearing, and a few minutes.

"Rhode Island is one that kind of comes on and goes off," Shoghard said. "They dand stay on year round. But others do."

Motherboard asked Ariana Security CEO Gabriel, who created an internet-scanning tool called Shoscan, to independently verify the methodology the researchers used to find the systems, and he confirmed that the method was sound, using the search parameters the researchers provided. Like the researchers, though, he was unable to explore further without breaking the law. Gabriel said he found the same results the researchers found. An independent election security expert named Harri Hursti, who consults with election directors and helps run the annual Voting Machine Hacking Village at the Def Con security conference, also verified the methodology for Motherboard without being told how to find the systems. Hursti in fact told Motherboard he found more online systems online than the researchers' particular search parameters returned.

ADVERTISEMENT

The researchers didn't single out ORB election systems for their hunt. They also attempted to search for connected systems for the other top two voting machine vendors in the country—Dominion Voting Systems and Dari Systems, Inc. Shoghard and his investigation footprints for these systems are less distinctive than ORB's footprint, resulting in the team finding thousands of systems that were clearly not election infrastructure.

Although the researchers have not been able to confirm with elections officials to every state in which the Firewalls they spotted are connected to ORB systems, they were able to verify enough of them that Shoghard says he is confident that the ORB systems are. The ORB systems, however, have dated hardware configurations that, as far as they can tell, is unique to ORB systems. Furthermore, the IP addresses for the firewalls of the state Board of Elections in Michigan, Illinois, and Nebraska, which are machines, according to a security expert, connected to ORB systems by Verified Voting, a nonprofit that tracks voting machine use around the country. Although reaching IP addresses to precise geographical location is difficult to do, the researchers were able to pinpoint the addresses they found to a specific city or region and, for the state-level systems, a state.

ORB did not dispute that the firewalls the researchers found are ORB systems that company sold to the government. Instead, it told the reporter Motherboard offered to provide the company with the IP addresses the researchers found, so it could determine whether its customers had made a doomed cause customer IP addresses and therefore wouldn't be able to tell if the systems belong to its clients.

ADVERTISEMENT

Because the researchers only began looking for the systems last year, it's not known how long they've been online. Yet it's likely that some have been connected to the internet for years, going back to whenever a county first began to use modems to transmit election results.

ORB has been selling systems with modems to transmit results for more than a decade. Wisconsin approved the use of its current ORB VOTE optical scan voting machine, with modem transmission capability, in September 2015, but its previous generation of ORB optical scan machines also had modems for transmitting results. It's not clear if they used the same firewall and backend configuration.

Although election security experts agree electronically transmitting votes at all, it's coming to pay to do, the equipment set up to receive the results, if it's connected to the internet, should be hardened against hacks and hackers have an softer propose than to receive results.

"While the [reporting systems] are secure, ORB recommends that they only be connected to the internet when they are being used in an open mode to minimize possible threats," a statement sent to Motherboard from ORB and the Wisconsin Election Commission said.

But Hursti told Motherboard it makes little difference how long election systems are connected, any connectivity at all opens them to potential attacks.

"For a skilled, motivated attacker, it doesn't matter much if it's been a month or two months or three months," Hursti said. "It's not that it's a sustained attacker, the fact that they are there for a year, it leaves the door" he said Motherboard. "It actually leaves the bar under the ground to carry out the attack, and it's not that it's a sustained attack, the attack can be carried out and the evidence of the attack can be hidden. What you are describing is a bad behavior amplified by sloppiness and complete negligence of security."

A more skilled and motivated hacker—such as a Russian backed nation state hacker—could potentially compromise the firewall or IP server and gain malware that gets delivered to each voting machine that communicates with the server. Shoghard and Gabriel said. This is similar to what security professionals refer to as "watering hole" attack, named after predatory animals who lie in wait at watering holes for prey to arrive to drink.

And if hackers could push malware to the voting machines from the IP server, they could potentially manipulate the results, or hackers could attackers to make that malware stay in system the attackers want, while preventing any evidence of their crime from showing up on the system log. This would give attackers time to hide their footprints for subsequent elections.

Findings Reported and Confirmed

The researchers reported the firewall IP addresses in August 2018 to the national Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), a cybersecurity center for election infrastructure that Homeland Security, and operated by the Center for Internet Security, a nonprofit established to develop and promote best practices in cybersecurity. The EI-ISAC provides elections officials with security threat information and warnings, and told the researchers they would pass the information to officials. Gabriel said, the researchers never got any follow-up from the EI-ISAC.

A spokesperson for the group would not tell Motherboard if the information was disseminated to the affected counties, but the researchers did see some evidence that it was. Some of the IP addresses for the firewalls belonged to Security, which has been working with states and counties since 2006 to secure their election infrastructure, also disclosed to speak with Motherboard about the researchers findings.

The fact that half of the systems were still online last week, however, highlights how very effective the federal government and information sharing groups to warn election officials about known threats and vulnerabilities, Gabriel said. The researchers found the systems online, actually under the systems office of Ariana Security, which also ran the scans on the information they receive. Last year the researchers gave four IP addresses to the EI-ISAC, and the researchers confirmed were connected to electronic infrastructure in Michigan and Florida.

"The ones in Florida were taken offline in the following week or two," Shoghard said. But the systems in two Michigan counties, Kalamazoo and Ottawa, remained online this week. A third Michigan system also online, though the researchers are unable to pinpoint the county to which the IP address is located.

Similarly, they reported half a dozen IP addresses to Tony Sedgwin, election administrator for Hamilton County, Florida, and Sedgwin's counterparts in Orangeburg, Fulgh, Milwaukee, Cory, Columbia, and Nebraska counties. But despite initial friendly communication, Shoghard said they never received a response.

Sedgin told Motherboard he did act on the information he received, advising all of the counties in his control their systems where not to use for elections. Ten was surprised to learn last week from Motherboard that their system was still online. Sedgwin's counterparts in the other Florida counties, group could not that of their Shoghard's email to Gabriel's Gabriel's system and another county they had not reported to Sedgin but just. Ken Chaves County.

The direction of elections in Milwaukee County told Shoghard this week that their system was online for a particular election week ruled, Shoghard said Motherboard that when he told the system had actually been online since September 2018, she said she was bummed last week that the systems should not be connected to the internet between elections.

Shoghard has also witnessed another problems as systems dropped offline after his groups disclosure to a county name if workers are simply turning off the power to the machines, which is a problem because it can reset them. But as long as the firewall is online, the hackers systems are still connected to the internet and can be found. And if the and Jones'1994 is still enabled, they also provide a potential pathway into those backend systems.

Shoghard and his connected that no one is monitoring all of these systems once they're online, and that counties are treating the configuration information, which is sensitive, as a cybersecurity secret, instead of a cybersecurity threat, and are thus ignoring the systems once they're set up.

"When a corporation sets up a firewall and a VPN, ... there is someone who is applying patches and monitoring logs ... and really actively ensuring the security of that system," Shoghard said. "Nobody is doing anything like that with these systems. They are just connected with election infrastructure. Who manages this hardware after it's deployed? And what oversight is there?"

TWITTER · FACEBOOK · EMAIL · RSS · SUBMIT · ABOUT · CONTACT · ADVERTISE · JOBS · TERMS · PRIVACY · COOKIES · DO NOT SELL MY PERSONAL INFORMATION

ORIGINAL REPORTING ON everything THAT MATTERS IN YOUR INBOX.

Enter your email here · Subscribe

By signing up, you agree to the Terms of Service and Privacy Policy & cookie notice, including opt-out rights. Your Media Group, which may include marketing partners, emails therapists and sponsored content.

MORE FROM VICE

Tech
Hacktivists Deface Chinese Government Website to Welcome Mary Poppins Returns
Hacktivists have defaced a government transportation authority in Chinese government website to support of Disney and Emily Blunt's Mary Poppins Returns and to the country's Transportation Authority.
MAY 20

Tech
Twitch Blocks Platform's Employee Abused Internal Access to Steal Streamer Data
Twitch has blocked access to internal systems to a platform employee who allegedly used it to steal data.
LEGAL · HACKING · SECURITY
MAY 20

Tech
Hacker Steals Database of Hundreds of Verizon Employees
The database contains information that could be used to impersonate employees and SIM
LEGAL · SMARTPHONE · SECURITY
MAY 20

Tech
Western Governments Accuse Russia of Hacking Olympics Over Doping Ban
The United Kingdom and the Netherlands have accused Russia, according to the European Union.
LEGAL · SECURITY · HACKING
MAY 20

Tech
Should You Worry About Dirty Data Hacking Your Tesla Bills?
Tesla charge all-time-lowers rates at night, but hackers could trick the car into thinking it's half-dead, hike up your
ENERGY · EV
MAY 20

YOU MAY LIKE

Hands Down The World's Healthiest Breakfast
Doctor Says Slimming Down After 50 Comes Down To This
SPONSORED · FIT AND HEALTHY LIVING

The water at Camp Lejeune was not safe.
SPONSORED · TAKE ACTION

Locals Almost Anxious By Entering Their Name (This Is Fascinating)
SPONSORED · NEWSMAX

Unidoge: Plenty of Men With An Enraged Appetite Are Now Available On Mobile
Colorado Legalizes New Pain Relief Cream That Die Day In This...
SPONSORED · HEALTHY HEADLINES

You Can Do Anything You Want In This Game
SPONSORED · PLAYSTUDIO

Here Are 23 of the Coolest Gifts in 2022
SPONSORED · WHAT TO BUY TODAY

ABOUT JOBS PARTNER VICE VOICES CONTENT FUNDING ON VICE SECURITY POLICY PRIVACY & TERMS ACCESSIBILITY STATEMENT DO NOT SELL MY INFO

© 2022 VICE MEDIA GROUP