Twitter Thread by Jewhadi™



Jewhadi™
@JewhadiTM



August 2019:

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

https://t.co/upYeltANXG

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

But a group of election security experts have found what they believe to be nearly three dozen backend election systems in 10 states connected to the internet over the last year, including some in critical swing states.

These include systems in nine Wisconsin counties, in four Michigan counties, and in seven Florida counties—all states that are perennial battlegrounds in presidential elections.

Some of the systems have been online for a year and possibly longer. Some of them disappeared from the internet after the researchers notified an information-sharing group for election officials last year.

But at least 19 of the systems, were still connected to the internet this week, 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 election systems.

The rest are still unconfirmed, but the fact that some of them appeared to quickly drop offline after the researchers reported them suggests their findings are on the mark.

“In some cases, [the vendor was] in charge [of installing the systems] 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."

The systems the researchers found are made by Election Systems & Software (@essvote), the top voting machine company in the country.

They are used to receive encrypted vote totals transmitted via modem from ES&S voting machines on election night, in order to get rapid results that media use 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 an election, poll workers remove these and drive them to county election offices.

But some counties want to get their results faster, so they use wireless modems, either embedded in the voting machines or externally connected to them, to transmit the votes electronically.

The system that receives these votes, called an SFTP server, is connected to the internet behind a Cisco 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 the transmission, and then for long enough after an election to transmit the votes.

But 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 fake results to the FTP server, depending on how securely the ES&S system authenticates the data.

Although the election results that are transmitted via modem are unofficial—official votes are taken directly from the voting machine memory cards when they arrive at county offices—

— a significant discrepancy between the unofficial tallies and the official ones would create mistrust in the election results and confusion about which ones were accurate.

But connected to the firewalls are even more critical backend systems—the election-reporting module that tabulates the unofficial votes as well as the official ones, and the election-management system that is used in some counties to program voting machines before elections.

Gaining access through the firewall to these systems could potentially allow hackers 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 ES&S documents posted online in various counties show that these critical backend systems are connected to the firewall, and ES&S also confirmed that this is the correct architecture in counties that want to transmit results electronically.

ES&S has long insisted that election-management systems are air-gapped—that is, not connected to the internet or connected to any other system that is connected to the internet—and the company insists that the diagram it provided isn't showing them connected to the internet.

"There's nothing connected to the firewall that is exposed to the internet," Gary Weber, vice president of software development and engineering for @essvote, told Motherboard. "Our [election-management system] is not pingable or addressable from the public internet."

This makes them invisible to bad actors or unauthorized users, he said.

But Skoglund said this "misrepresents the facts." Anyone who finds the firewall online also finds the election-management system connected to it.

"It is not air-gapped. The EMS is connected to the internet but is behind a firewall," Skoglund said. "The firewall configuration [that determines what can go in and out of the firewall]… is the only thing that segments the EMS from the internet."

And misconfigured firewalls are one of the most common ways hackers penetrate supposedly protected systems. The recent massive hack of sensitive Capital One customer data is a prime example of a breach enabled by a poorly configured firewall.

"If they did everything correctly [with the ES&S systems] as they say they do, there is no danger," Robert Graham, CEO of Errata Security, told Motherboard.

"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. And the fact that [election officials are] saying they aren't on the internet and yet they are on the internet shows us that we have every reason to distrust them."

Even proper configurations won't secure a firewall if the firewall software itself has security vulnerabilities that allow intruders to bypass all the authentication checks, whitelisting rules, and other security parameters set in the firewall's configuration file.

"If this system hasn't been patched and has a critical vulnerability… you may be able to subvert any kind of security scheme that you've put in place," Skoglund told Motherboard.

Senator Ron Wyden (D-Oregon) said the findings are "yet another damning indictment of the profiteering election vendors, who care more about the bottom line than protecting our democracy."

It's also an indictment, he said, "of the notion that important cybersecurity decisions should be left entirely to county election offices, many of whom do not employ a single cybersecurity specialist."

“Not only should ballot tallying systems not be connected to the internet, they shouldn’t be anywhere near the internet,” he added.

What’s not generally known by the public about @essvote systems is that the company’s entire configuration for transmitting election results—from the modem to the SFTP server—is NOT CERTIFIED BY THE ELECTION ASSISTANCE COMMISSION (EAC).

The EAC oversees the testing and certification of voting equipment at the federal level. ES&S voting machines are tested and certified, but the transmission configuration isn’t. The labs test them for functionality to make sure they transmit votes, and that’s it.

In marketing literature, ES&S highlights the certified parts of its election system in blue and labels them "EAC Certified Configuration." The uncertified part is highlighted in white and labeled "Extended Configuration."

.@essvote told Motherboard that instead of federal certification, his company has focused on working with officials in states that allow modem transmission to test and certify the configuration under their own state certification programs.

This is said to include a security assessment of the configuration. Asked which states do these security assessments, he cited Wisconsin, Florida, and Minnesota.

But someone familiar with Wisconsin’s certification testing, who spoke on condition of anonymity, told Motherboard it doesn’t include a security assessment of the modem transmissions and configuration.”