STATE AFFAIRS
WISPOLITICS
Wisconsin's Premier Political News Service

Review finds Wisconsin voting equipment at times connected to internet, potentially vulnerable

Posted on Saturday, Sep 14, 2019

By Patrick Poblete
WisPolitics.com

Vital election equipment in at least seven Wisconsin counties has been connected to the internet, in some cases for nearly a year at a time, despite Wisconsin elections officials and voting machine vendors repeatedly claiming the devices cannot be hacked because they are not connected to the web.

A group of election security experts who went looking for vulnerabilities to check claims of vendors found the connections and warned the Wisconsin Elections Commission ahead of the 2018 midterm elections. But state officials failed to notify all but one of the counties.

WEC spokesman Reid Magney said the commission was “dealing with a number of issues” at the time and was “not sure that this was the most pressing.” He also insists that there is no evidence of a hack and said voting machines have been audited back against the original paper ballots filled out by voters.

But election security expert Doug Jones told WisPolitics.com that securing the voting systems in question should have been WEC’s top priority.

The systems are only supposed to be connected to the internet for brief periods of time to test transmission and receive vote totals. But the researchers found in some counties the systems were left connected for long periods, leaving the door open to a hacker intercepting unofficial results, sending fake results, or installing malware that corrupts the computers used to program voting machines and by extension voting machines themselves.

“This could give a run-of-the-mill hacker complete control of the reported outcome,” said Jones, a computer science professor at the University of Iowa who specializes in electronic voting security. He was not part of the research team.

The researchers' initial sweep found Elections Systems & Software voting machines in six counties were connected to the internet and dangerously vulnerable to hackers: Outagamie, Dodge, Milwaukee, St. Croix, Columbia and Waukesha counties. A later check then found Eau Claire County also had equipment connected to the internet.

Of that group, only county clerks from Dodge and Waukesha counties returned emails from WisPolitics.com requesting comment on this story. Dodge County Clerk Karen Gibson said in an email WisPolitics.com's conversations with WEC and ES&S "covered this topic" and did not respond to follow-up questions. Waukesha County Clerk Meg Wartman said in an email reports that Waukesha County voting machines are connected to the internet are "incorrect" but did not immediately respond to a follow-up email from WisPolitics.com containing ES&S documentation contrary to her claim.

ES&S spokeswoman Katina Granger told WisPolitics.com it is "erroneous" to suggest the vendor's voting machines are connected to the internet. Instead, Granger said the modems transmit the unofficial results "over secure communication channels."

"It's a gaslighting of the public"

The group of elections security researchers began the hunt for online voting machines in July 2018 after hearing repeatedly from local elections officials and voting machine companies that election equipment is safe from hacking because it is not connected to the internet. The group was particularly curious about modeming, or transmitting via cellular networks or landlines, of unofficial elections results after the polls close.

The researchers uncovered nearly three dozen elections systems across 10 states that were connected to the internet. They shared the information with freelance journalist Kim Zetter, who published their findings in the tech publication Motherboard. Kevin Skoglund served as the spokesman for the research team, described in Zetter's story as being comprised of 10 "long-time security professionals and academics with expertise in election security." Skoglund provided information to WisPolitics.com for this story, but declined to be interviewed on the record.

The researchers believed the modeming of results was the first indication that undercut the claims that voting machines are not connected to the internet.

In the case of ES&S DS200 optical ballot scanner and vote tabulators, Magney said election workers switch the machines into what's known as "reporting mode" after polls close. At that point, Magney says, the machines print out a paper record of the results "like a cash register receipt" and deliver the unofficial results to the county through encrypted outgoing cellular phone calls.

"Every expert you talk to will tell you, 'Yes, cellular traffic goes through the internet,'" said Zetter in an interview with WisPolitics.com

Magney conceded that after the results were printed "there is, at that point, a connection to the internet."

While election device vendors dispute that categorization, Zetter acquired a graphic within an ES&S document that the vendor supplied to Rhode Island in 2015 showing modem connections going over the internet.

That document and Magney's statement runs counter to at least five statements on the ES&S website, as well as a bevy of documents the company has provided to states and public statements the company's representatives have given before the WEC.

"The vendors know their systems are connecting through the internet, even if their election official customers do not realize it or continue to insist to the public that the systems are not connected to the internet," Skoglund said in the Motherboard story.

"It's a gaslighting of the public and of elections officials," said Zetter, who compared public messaging from voting machine vendors to the propaganda-peddling Ministry of Truth in George Orwell's dystopian novel "Nineteen Eighty-Four.''

A post on WEC website categorized under "Voting Equipment Security" claiming that "voting equipment is not connected to the internet" has also been up for nearly three years at the least, according to the internet archive site Wayback Machine.

"That was like saying that the Golden Gate Bridge isn't connected to San Francisco"

Sending the unofficial results over the internet was only the tip of the iceberg, according to the researchers.

With the knowledge in hand that vote tabulators were in fact connecting to the internet, Skoglund’s group set to the task of developing a system that could identify nationally the backend internet-connected elections systems that receive the transmitted votes.

That system, known as an SFTP server, is connected to the internet but sits behind a firewall, software that examines traffic coming in and only allows authenticated systems through.

After a member of the group found IP addresses identifying ES&S firewalls in publicly available documents from Rhode Island, the researchers were able to use a specialized search engine to identify at least 35 internet-connected systems nationwide. Nine were spread across six Wisconsin counties.

Also behind the ES&S firewall nationally are two critical backend systems: the reporting system that tabulates votes and the election management systems that programs the voting machines to read the ballots.

On election nights, the reporting system collects the encrypted votes the voting machines have deposited on the SFTP server by reaching through the firewall to examine the server for new files every few minutes. If new files have arrived, the reporting system decrypts them to read the votes inside and tabulates them.

In plain language, Jones explains, essentially all elections infrastructure is online — from computers that program voting machines and by extension voting machines themselves to the server that receives the votes to reporting systems that decrypt and tabulate the tally.

While Magney touted the security of the firewall, ES&S claims any equipment behind that firewall is not connected to the internet.

But according to Zetter, “It’s a definition that is unique to ES&S, and of course it serves their purpose of wanting to insist that the systems aren’t connected to the internet.”

“That was like saying that the Golden Gate Bridge isn’t connected to San Francisco, because there’s a toll bridge that you have to cross to get to the bridge,” she said, relaying a metaphor she found on Twitter. “The toll bridge doesn’t prevent someone from getting on the bridge. All it does is say you have to pay something to get on this bridge."

Similarly, Zetter says, a firewall on backend elections systems regulates what systems can contact that machine through the internet. If that firewall is up-to-date and well-maintained, the system behind it is secure.

But far too often that's not the case.

Both Jones and Zetter highlighted the recent "massive" hack of Capital One's sensitive customer data as an example of a breach via poorly established firewall.

"There's a long list of ways that firewalls are done poorly and problematically; that's why we have breaches all the time in the news," Zetter said.

"They're not even gonna know that their system is wide open"

At the top of the list of ways firewalls can be breached is a failure to patch them in a timely manner once security flaws have been identified. And that's exactly what happened in Wisconsin.

Zetter reported in her story that firewalls created by tech giant Cisco protecting ES&S voting systems in Wisconsin failed to receive a patch released in January 2018 for a critical vulnerability until July 2018. That was six months after the vulnerability had been made public, and the patch was released.

"That was a lengthy process, and we're just talking about one vulnerability here," she said. "There are multiple vulnerabilities discovered in products all the time, and unless someone is actually monitoring when a patch has been available and when a vulnerability has been announced, they're not even gonna know that their system is wide open.

"And that's only addressing it after it is actually publicly known. Cisco didn't know about that vulnerability until someone reported it to them. So then the question is how long did that vulnerability exist in those firewalls used by ES&S systems before anyone actually publicly knew there was a vulnerability and then could create a patch."

Because the firewall is certified by the federal Elections Assistance Commission, any updates or patches must be tested by the EAC in order to gain certification. Once the patch is approved at the federal level, the EAC sends states an “engineering change order.” Magney attributed the delay in applying the patch largely to the certification process at the federal level.

Zetter says delays caused by ECOs are fairly common. But she said the length of time systems in the state were vulnerable and ES&S’ response to the vulnerability when she contacted them in February 2018 were concerning.

“I got the impression that they weren’t aware of the vulnerability at all, even though they implied to me that they were in the process of working with clients to get them patched,” she said.

Granger did not respond to an email from WisPolitics.com asking when ES&S discovered the vulnerability. But she did tell WisPolitics.com that in all seven counties identified by Skoglund’s group, “ES&S technicians installed and configured election management systems, including firewalls… during installation and upgrade activities.”

“You’ve subverted the election”

Skoglund’s work and Zetter’s reporting conclude election systems in Wisconsin were online during a period in which a critical vulnerability was publicly known and not fixed.

Still, Magney insists there is no evidence that Wisconsin elections systems have been hacked.

“Anything that was available during 2018 has been audited,” Magney says, a process that compares the official vote tally back against the original paper ballots filled out by voters.

But both Zetter and Jones said the voting system vulnerabilities could have been exploited by hackers in ways that have yet to fully come to fruition.

Zetter described to WisPolitics.com a hack known as a “watering hole” attack, in which a hack penetrates the firewall through a known vulnerability and deposits malware that sits dormant on the SFTP server and waits for the voting machine to contact it. Once that happens, Zetter said, the malware can be deposited back on the voting machine via the election management system, which also sits behind the firewall.

“Once you’ve got something on that voting machine, you could alter the voting machine, you can alter the modem on that voting machine, all that,” Zetter said.

Such an attack would spoil unofficial results, but leave the official vote tally untouched. But Jones says discrepancies between the two tallies would cause turmoil and raise doubts among the public about the integrity of American elections.

But Zetter says it’s not only the unofficial results at risk.

Because the elections management system — which programs the voting machines before elections and handles official results that come in on election night through memory cards — is connected to the firewall, it is vulnerable to attack.

Zetter said paper ballots marked manually by a voter are the ultimate insurance against hackers. A so-called “risk-limiting audit” — in which the paper ballots are compared back against official election results — could detect if a hack, or glitch in the system, had caused vote tabulation devices to miscount and ensure the will of voters is represented accurately.

Zetter found in the course of her reporting, though, that “some of those counties actually did do a manual examination of the paper ballots and others simply just ran those ballots right through the same software again.”

Magney in an email strongly pushed back on the notion that this practice is problematic, telling WisPolitics.com that “all the voting equipment used in the recount was reprogrammed.”

But Zetter said reprogramming the machines doesn’t do anything to solve the problem since the elections management systems used to do the reprogramming are connected to the firewall and thus vulnerable to hackers.

“First thing the next morning, we were on the phone to all of the counties”

Just over a year after the researchers first began hunting for online systems, Zetter was wrapping up her story and reached out to the WEC to follow up on the researchers’ warning.

She reached out to Tony Bridges, WEC’s security lead and the elections official to whom Skoglund had initially reported his group's finding. It's at this point Zetter's account begins to differ drastically from the WEC's version of events.

Zetter reported in her story that Bridges said he acted on the information he received from Skoglund roughly 12 months before, "advising all of the counties to disconnect their systems when not in use for elections." Zetter reported Bridges was surprised to learn that a number of counties still had systems online and contacted them again, at which point Skoglund's group saw all but Milwaukee and Eau Claire counties drop off its monitoring system. Milwaukee County was in the midst of a special election at the time while Eau Claire County had not been identified in the initial sweep.

Skoglund told Zetter that when he reached out to a Milwaukee County elections official earlier this month to inform her that her system had actually been online since September 2018, "she said she only learned the week before that the systems should not be connected to the internet between elections."

The other account, told by Magney to WisPolitics.com, suggests elections officials scrambled in advance of a media spotlight.

Magney said when Bridges was initially alerted by Skoglund about the vulnerability in the later summer of 2018, "he alerted someone on our staff about that" and "reached out to at least one county clerk" but said Bridges does not recall "which one he talked to."

The WEC spokesman later clarified in an email that members of the public contact WEC regularly with concerns about selection security.

"However, it is not always clear whether their concerns are based on credible information, misinformation or misunderstandings," he said.

Still, Magney acknowledged that it was only after Zetter reached out on July 31, 2019, shortly before the Aug. 8 story and made it clear to Bridges that there would be press coverage of the vulnerabilities that WEC officials took action.

"First thing the next morning, we were on the phone to all of the counties that were identified asking them about what their situation was," Magney said.

Magney said all seven county clerks were advised to immediately unplug the systems' routers to make them inaccessible from the internet.

“Six of the seven did so. Milwaukee County was testing its equipment for an upcoming special election, after which it also unplugged its router,” Magney said in an email.

Magney conceded that Bridges told Zetter he had contacted the six counties, but later became unsure and “felt he had misspoke” when recounting events that had taken place roughly a year before the conversation. Magney said Bridges clarified with Zetter that he may not have contacted all the counties.

WEC officials also learned in August that ES&S had recommended in October 2018 that counties should follow the best practice of unplugging routers used to accept unofficial results transmissions from polling places when they are not being tested or used. Critics see that as yet another example that appears to undercut the vendor’s claim that their systems are not online. But several counties never received that memo.

Granger did not respond to an email from WisPolitics.com asking why the memo wasn’t distributed to all ES&S customers.

But at the end of the day, Magney said, the WEC is not responsible for the security of county and municipality voting systems.

“Counties and municipalities have historically been responsible for the security of their own computer systems and networks, including voting equipment and systems,” Magney said. “Monitoring local security has never been part of WEC’s statutory duties, but the agency is now exploring ways it can help its local election partners with that task.”

“It shouldn’t be on the internet.”

Zetter and Jones reserved a majority of their scorn for the device vendors and acknowledged Magney is correct when he says WEC officials were “dealing with a number of issues” when Skoglund first reached out to inform them of the vulnerabilities. Jones compared running an election to “fighting a war.”

“You’ve got problems coming out all over the place, and you have to do really short-term decisions, prioritizing issues to deal with, with limited resources,” he said. “I am not at all shocked that this particular issue was pushed onto a back burner with short lead time and short resources.

“If you have a choice between failing to open the polls and dealing with this issue, you better open the polls.”

Zetter agreed, telling WisPolitics.com that elections officials across the country are often overloaded. But that, she says, underlies the need for voting systems to be taken offline.

“You shouldn’t be putting something on the internet if you’re too busy to address it when problems come up, if you’re too busy to maintain it properly, if you’re too busy to configure it securely,” she said.

“It shouldn’t be on the internet.”

See the Motherboard story:
https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials

See the ES&S FAQ page:
https://www.essvote.com/faqs/

See the ES&S security information page:
https://www.essvote.com/feature/security/

See the WEC Voting Equipment Security page:
https://elections.wi.gov/elections-voting/voting-equipment/security