New election systems use vulnerable software

July 13 2019, by Tami Abdollah

In this June 13, 2019, photo, Steve Marcinkus, an Investigator with the Office of the City Commissioners, demonstrates the ExpressVote XL voting machine at the Reading Terminal Market in Philadelphia. An analysis by The Associated Press has found that the vast majority of the nation's 10,000 election jurisdictions will be managing their elections on Windows 7 or an even older operating system. (AP Photo/Matt Rourke)

Pennsylvania's message was clear: The state was taking a big step to keep its elections from being hacked in 2020. Last April, its top election official told counties they had to update their systems. So far, nearly 60% have taken action, with $14.15 million of mostly federal funds helping counties buy brand-new electoral systems.

But there's a problem: Many of these new systems still run on old software that will soon be outdated and more vulnerable to hackers.

An Associated Press analysis has found that like many counties in Pennsylvania, the vast majority of 10,000 election jurisdictions nationwide use Windows 7 or an older operating system to create ballots, program voting machines, tally votes and report counts.

That's significant because Windows 7 reaches its "end of life" on Jan. 14, meaning Microsoft stops providing technical support and producing "patches" to fix software vulnerabilities, which hackers can exploit. In a statement to the AP, Microsoft said Friday it would offer continued Windows 7 security updates for a fee through 2023.

Critics say the situation is an example of what happens when private companies ultimately determine the security level of election systems with a lack of federal requirements or oversight. Vendors say they have been making consistent improvements in election systems. And many state officials say they are wary of federal involvement in state and local elections.

It's unclear whether the often hefty expense of security updates would be paid by vendors operating on razor-thin profit margins or cash-strapped jurisdictions. It's also uncertain if a version running on Windows 10, which has more security features, can be certified and rolled out in time for primaries.

"That's a very serious concern," said J. Alex Halderman, a University of Michigan professor and renowned election security expert. He said the country risks repeating "mistakes that we made over the last decade or decade-and-a-half when states bought voting machines but didn't keep the software up-to-date and didn't have any serious provisions" for doing so.

The AP surveyed all 50 states, the District of Columbia and territories, and found multiple battleground states affected by the end of Windows 7 support, including Pennsylvania, Wisconsin, Florida, Iowa, Indiana, Arizona and North Carolina. Also affected are Michigan, which recently acquired a new system, and Georgia, which will announce its new system soon.

"Is this a bad joke?" said Marilyn Marks, executive director of the Coalition for Good Governance, an election integrity advocacy organization, upon learning about the Windows 7 issue. Her group sued Georgia to get it to ditch its paperless voting machines and adopt a more secure system. Georgia recently piloted a system running on Windows 7 that was praised by state officials.

If Georgia selects a system that runs on Windows 7, Marks said, her group will go to court to block the purchase. State elections spokeswoman Tess Hammock declined to comment because Georgia hasn't officially selected a vendor.

The election technology industry is dominated by three titans: Omaha, Nebraska-based Election Systems and Software LLC; Denver, Colorado-based Dominion Voting Systems Inc.; and Austin, Texas-based Hart InterCivic Inc. They make up about 92% of election systems used nationwide, according to a 2017 study . All three have worked to win over states newly infused with federal funds and eager for an update.

U.S. officials determined that Russia interfered in the 2016 presidential election and have warned that Russia, China and other nations are trying to influence the 2020 elections.

Of the three companies, only Dominion's newer systems aren't touched by upcoming Windows software issues—though it has election systems acquired from no-longer-existing companies that may run on even older operating systems.

Hart's system runs on a Windows version that reaches its end of life on Oct. 13, 2020, weeks before the election.

ES&S said it expects by the fall to be able to offer customers an election system running on Microsoft's current operating system, Windows 10. It's now being tested by a federally accredited lab.

For jurisdictions that have already purchased systems running on Windows 7, ES&S said it will be working with Microsoft to provide support until jurisdictions can update. Windows 10 came out in 2015.

Hart and Dominion didn't respond to requests for comment.

Microsoft usually releases patches for operating systems monthly, so hackers have learned to target older, unsupported systems. Its systems have been ground zero for crippling cyberattacks, including the WannaCry ransomware attack, which froze systems in 200,000 computers across 150 countries in 2017.

For many people, the end of Microsoft 7 support means simply updating. However, for election systems the process is more onerous. ES&S and Hart don't have federally certified systems on Windows 10, and the road to certification is long and costly, often taking at least a year and costing six figures.

ES&S, the nation's largest vendor, completed its latest certification four months ago, using Windows 7. Hart's last certification was May 29 on a Windows version that also won't be supported by November 2020.

Though ES&S is testing a new system it's unclear how long it will take to complete the process—federal and possible state recertification, plus rolling out updates—and if it will be done before primaries begin in February.

Election administrators notoriously suffer from insufficient resources. Recently, many jurisdictions splurged on new election systems, some using their portion of $380 million in federal funds provided to states.

Counties in South Dakota, South Carolina and Delaware all recently bought election systems, while many others are evaluating purchases.

The use of election systems that still run on Windows 7 "is of concern, and it should be of concern," said U.S. Election Assistance Commission Chair Christy McCormick. EAC develops election system guidelines.

McCormick noted that while election systems aren't supposed to be connected to the internet, various stages of the election process require transfers of information, which could be points of vulnerability for attackers. She said some election administrators are working to address the problem.

Officials in Pennsylvania, Michigan and Arizona say they have discussed the software issue with their vendors. Other states mentioned in this story didn't respond to AP requests for comment.

Pennsylvania elections spokeswoman Wanda Murren said contract language allows such a software upgrade for free. Arizona elections spokeswoman C. Murphy Hebert said ES&S has also assured the state

that it will provide support to counties for an upgrade.

Susan Greenhalgh, policy director for the advocacy group National Election Defense Coalition, said even the best scenario has election administrators preparing for primaries while trying to upgrade their systems, which is "crazy." Her group shared its concerns about Windows 7 with AP.

Certification, which is voluntary at the federal level but sometimes required by state laws, ensures vendor software runs properly on operating systems they're tested on. But there is no cybersecurity check and the process often fails to keep up with rapidly changing technology.

Kevin Skoglund, chief technologist for Citizens for Better Elections, said county election officials point to EAC and state certifications as "rock-solid proof" their systems are secure, but don't realize vendors are certifying systems under 2005 standards.

Local officials rely on vendors to build secure systems and EAC and the states to enforce high standards, Skoglund said.

After the AP began making inquiries, Sen. Ron Wyden, D-Ore., wrote McCormick asking what EAC, which has no regulatory power, is doing to address a "looming election cybersecurity crisis" that essentially lays the "red carpet" out to hackers.

"Congress must pass legislation giving the federal government the authority to mandate basic cybersecurity for election infrastructure," Wyden told the AP in a statement.

from https://phys.org/news/2019-07-election-vulnerable-software.html