Researcher finds Georgia voter records exposed on internet

June 15 2017, by Frank Bajak

This Sept. 22, 2016 file photo shows employees of the Fulton County Election Preparation Center in Atlanta test electronic voting machines. A security researcher disclosed a gaping security hole at the outfit that manages Georgia's elections. The lapse, which left the state's 6.7 million voter records and other sensitive files exposed to hackers, was first reported Wednesday, June 14, 2017, by the news site Politico. (AP Photo/Alex Sanz)

A security researcher disclosed a gaping security hole at the outfit that manages Georgia's election technology, days before the state holds a closely watched congressional runoff vote on June 20.

The security failure left the state's 6.7 million voter records and other sensitive files exposed to hackers, and may have been left unpatched for seven months. The revealed files might have allowed attackers to plant malware and possibly rig votes or wreak chaos with voter rolls during elections.

Georgia is especially vulnerable to such disruption, as the entire state relies on antiquated touchscreen voting machines that provide no hardcopy record of votes, making it all but impossible to tell if anyone has manipulated the tallies.

The true dimensions of the failure were first reported Wednesday by Politico Magazine . The affected Center for Election Systems referred all questions to its host, Kennesaw State University, which declined comment. In March, the university had mischaracterized the flaw's discovery as a security breach.

Logan Lamb, a 29-year-old Atlanta-based private security researcher formerly with Oak Ridge National Laboratory, made the discovery last August. He told The Associated Press he decided to go public after the publication last week of a classified National Security Agency report describing a sophisticated scheme, allegedly by Russian military intelligence, to infiltrate local U.S. elections systems using phishing emails.

The NSA report offered the most detailed account yet of an attempt by foreign agents to probe the rickety and poorly funded U.S. elections system. The Department of Homeland Security had previously reported attempts last year to gain unauthorized access to voter registration databases in 20 states—one of which, in Illinois, succeeded, though the state says no harm resulted.

It also emboldened Lamb to come forward with his findings. Lamb

discovered the security hole—a misconfigured server—one day as he did a search of the Kennesaw State election-systems website. There, he found a directory open to the internet that contained not just the state voter database, but PDF files with instructions and passwords used by poll workers to sign into a central server used on Election Day, said Lamb.

"It was an open invitation to anybody pretending to even know a little bit about computers to get into the system," said Marilyn Marks, an election-transparency activist whose Colorado-based foundation participated in a failed lawsuit that sought to bar the use of paperless voting machines in next week's election.
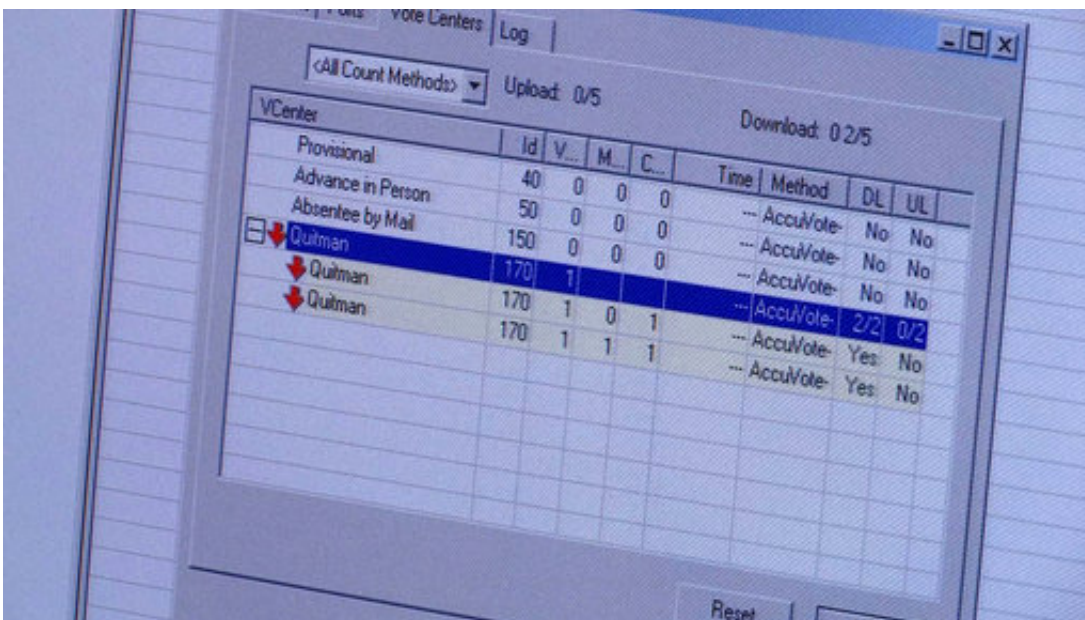
This Sept. 22, 2016 file photo shows the screen of an electronic voting machine during testing at the Kennesaw State University Center for Election Systems in Kennesaw, Ga. A security researcher disclosed a gaping security hole at the outfit that manages Georgia's elections. The lapse, which left the state's 6.7 million voter records and other sensitive files exposed to hackers, was first reported Wednesday, June 14, 2017, by the news site Politico. (AP Photo/Alex Sanz, File)

The directory of files "was already indexed by Google," Lamb said in an interview—meaning that anyone could have found it with the right search. Lamb said he notified the center's director, Merle King, who assured him the hole would be patched and who asked to keep his discovery to himself.

Politico reported that the center never notified the secretary of state's office, which oversees elections and contracts with Kennesaw State to manage the technology part. The Associated Press left a phone message and sent email to King seeking comment but he did not immediately respond.

Lamb said he decided not to disclose the problem at the time—mostly because he "didn't want to needlessly escalate things" prior to the Nov. 8 general election. But in March, a security colleague Lamb had told about the flaw, checked out the center's website and discovered that the vulnerabilities had only been partially fixed.

"We were both pretty floored," said Lamb.

The researcher, Chris Grayson, said he, too, was able to access the same voter record database and other sensitive files in a publicly accessible directory. Grayson contacted a friend who is a professor at Kennesaw State. Two days later, the FBI was called in to investigate.

It did not bring charges against either researcher, finding no evidence of illegal entry . "At the end of the day we were doing what we thought was in the best interest of the republic—informing the parties that needed to be privy to this sort of issue," said Grayson.

The special election next Tuesday will fill the seat vacated by

Republican Tom Price after he was named Health and Human Services Secretary. It has attracted national attention, including that of President Donald Trump, for whom it could be a bellwether.

First-time candidate Jon Ossoff is a Democrat with a national security background. His GOP opponent is former Georgia Secretary of State Karen Handel.

Citation: Researcher finds Georgia voter records exposed on internet (2017, June 15) retrieved 27 April 2024 from https://phys.org/news/2017-06-georgia-voter-exposed-internet.html