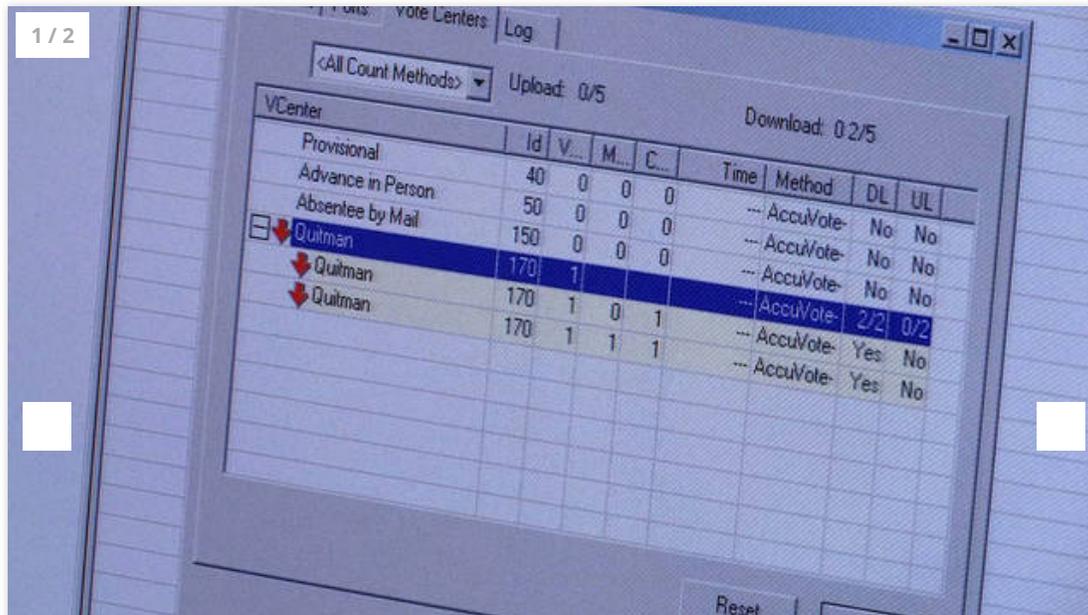TOP NEWS

Georgia election server wiped after suit filed

Associated Press
Posted October 26, 2017
October 26, 2017

*Updated October 26, 2017 7:54am*

ASSOCIATED PRESS

The screen of an electronic voting machine during testing, in Sept. 2016, at the Kennesaw State University Center for Election Systems in Kennesaw, Ga. A computer server crucial to a lawsuit against Georgia election officials was quietly wiped clean in July, just after the suit was filed.

A computer server crucial to a lawsuit against Georgia election officials was quietly wiped clean by its custodians just after the suit was filed, The Associated Press has learned.

The server's data was destroyed July 7 by technicians at the Center for Elections Systems at Kennesaw State University, which runs the state's election system. The data wipe was revealed in an email — sent last week from an assistant state attorney general to plaintiffs in the case — that was obtained by the AP. More emails obtained in a public records request confirmed the wipe.

The lawsuit, filed by a diverse group of election reform advocates, aims to force Georgia to retire its antiquated and heavily criticized election technology. The server in question, which served as a statewide staging location for key election-related data, made national headlines in June after a security expert disclosed a gaping security hole that wasn't fixed six months after he reported it to election authorities.
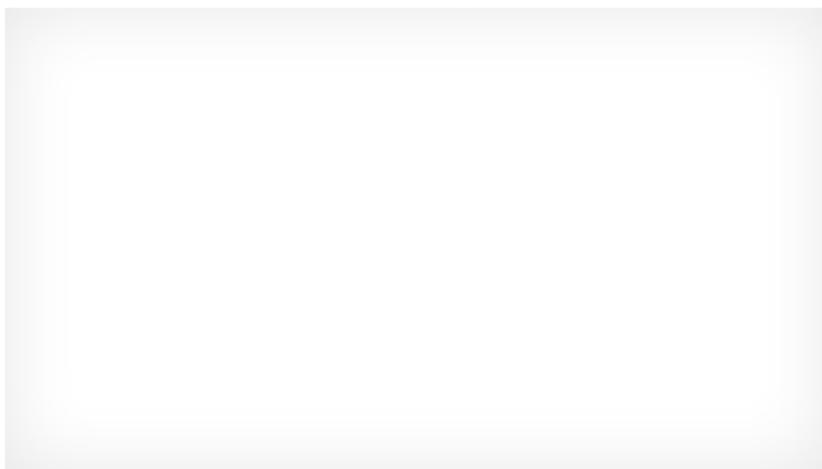
WIPED OUT

It's not clear who ordered the server's data irretrievably erased.

The Kennesaw election center answers to Georgia's secretary of state, Brian Kemp, a Republican who is running for governor in 2018 and is the main defendant in the suit. A spokeswoman for the secretary of state's office said Wednesday that "we did not have anything to do with this decision," adding that the office also had no advance warning of the move.

The center's director, Michael Barnes, referred questions to the university's press office, which declined comment.

Plaintiffs in the lawsuit, who are mostly Georgia voters, want to scrap the state's 15-year-old vote-management system — particularly its 27,000 AccuVote touchscreen voting machines, hackable devices that don't use paper ballots or keep hardcopy proof of voter intent. The plaintiffs were counting on an independent security review of the Kennesaw server, which held electronic poll book data and ballot definitions for counties, to demonstrate the system's unreliability.

Wiping the server clean "forestalls any forensic investigation at all," said Richard DeMillo, a Georgia Tech computer scientist who has closely followed the case. "People

who have nothing to hide don't behave this way."

STATE SECURITY

The server data could have revealed whether Georgia's most recent elections were compromised by malicious hackers. The plaintiffs contend that the results of both last November's election and a special June 20 congressional runoff— won by Kemp's predecessor, Karen Handel — cannot be trusted.

Possible Russian interference in U.S. politics, including attempts to penetrate voting systems, has been an acute national preoccupation since the Obama administration first sounded the alarm more than a year ago.

Kemp and his GOP allies insist Georgia's elections system is secure. But Marilyn Marks, executive director of the Coalition for Good Governance, a plaintiff, believes the server data was erased precisely because the system isn't secure.

"I don't think you could find a voting systems expert who would think the deletion of the server data was anything less than insidious and highly suspicious," she said.

J.Tom Morgan, a former Georgia prosecutor, said destruction of the drive would not be a criminal act unless it was in violation of a protective court order (It appears no such order was requested). But it could seriously damage the defendants' case, he said.

NOW YOU SEE IT, NOW YOU DON'T

It could still be possible to recover relevant information from the server.

The FBI is known to have made an exact data image of the server in March when it investigated the security hole. The email that disclosed the server wipe said the state attorney general's office was "reaching out to the FBI to determine whether they still have the image."

Atlanta FBI spokesman Stephen Emmett, responding to AP questions, would not say whether that image still exists. Nor would he say whether agents examined it to determine whether the server's files might have been altered by unauthorized users.

Other backups also appear to be gone. In the same email to plaintiffs' attorneys, assistant state Attorney General Cristina Correia wrote that two backup servers were also wiped clean on Aug. 9, just as the lawsuit moved to federal court.

FAILING TO SERVICE THE SERVER

A 140-page collection of Kennesaw State emails, obtained Friday by the Coalition for Good Governments via an open records search, details the destruction of the data on all three servers and a partial and ultimately ineffective effort by Kennesaw State systems engineers to fix the main server's security hole.

As a result of the failed effort, sensitive data on Georgia's 6.7 million voters — including social security numbers, party affiliation and birthdates — as well as passwords used by county officials to access elections management files remained exposed for months.

The problem was first discovered by Atlanta security researcher Logan Lamb, who happened across it while doing online research in August 2016. He informed the election center's director at the time, noting in an email that "there is a strong possibility your site is already compromised."

Based on his review of the emails, Lamb believes that electronic polling books could have been altered in Georgia's biggest counties to add or drop voters or to scramble their data. Malicious hackers could have altered the templates of the memory cards used in voting machines to skew results.

An attacker could even have modified "ballot-building" files to corrupt the count, said Lamb, who works at Atlanta-based Bastille Networks.

But it will be impossible to know for sure unless the FBI provides a copy of the server image for analysis.

✉ **Get the latest news by email**   Sign Up