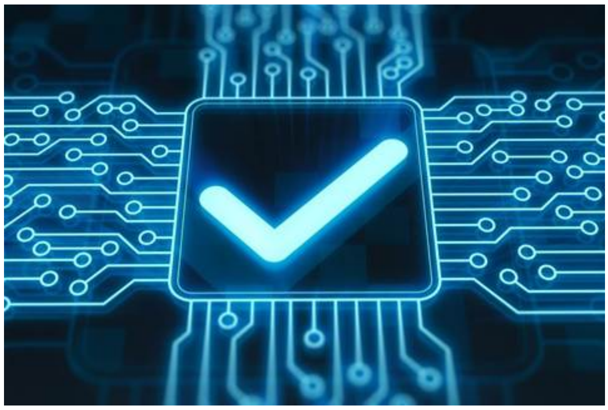
NSW Electoral Commission confirms iVote contains critical Scytl crypto defect

By Justin Hendry (/author/justin-hendry-1167397) on Mar 13, 2019 10:13AM

But declares it unaffected and safe for upcoming state election.



The NSW Electoral Commission has confirmed a critical defect found in the Swiss government's e-voting system allowing vote manipulation to take place is also present in the state's iVote system.

But the electoral body has stressed that its online voting platform is still safe to use in the state election later this month.

It follows new research on Tuesday that revealed a critical issue with the way the Swiss government's sVote system run by Swiss Post verified ballots cast in an election.

The cryptographic trapdoor (https://www.itnews.com.au/news/crypto-trapdoor-found-in-swiss-e-voting-system-520440) goes to the heart of the system, which like the NSW government's iVote system uses software from the Spanish vendor Scytl.

It allows a malicious authority to change votes without being able to detect that manipulation, which the researchers put down to the implementation of the Bayer and Groth proof mechanism.

But in a statement NSWEC said that, although "present in the iVote system", the identified "issue does not affect the use of iVote for the NSW state election".

…decrypted and c… ensure they cannot be connected to individual voters,” the Commission said.

“This is part of the process that ensures that iVote users have the same ability to cast a secret ballot as voters who use any other voting channel.”

“Scytl is working with the Commission to deploy a fix for the system this week.”

However it said that, unlike the Swiss Post system, the NSWEC “machine on which the mixnet runs is not physically connected to any other computer systems either within or outside the NSW Electoral Commission”.

“In order for this weakness to be an issue, a person would need to gain access to the physical machine. They would need all the right credentials and the right code to alter the software,” the Commission said.

iVote has been closed for ‘system maintenance’ since 5:30pm on Tuesday, which the NSWEC website puts down to "reports of an usability issue casting a vote using iVote".

The discovery of the cryptographic trapdoor in the Swiss government's and NSW government's e-voting systems highlights the importance of opening source code to the public.

This was a key recommendation of a recent review into the iVote system (https://www.itnews.com.au/news/review-finds-security-of-nsws-ivote-system-adequate-516184) by former secretary of the federal Attorney-General’s Department Roger Wilkins.

In January, the NSWEC invited individuals with a private or academic interest to review aspects of the iVote system source code prior to the election. This is in addition to its own private testing.