techworm.net

Programmer Rewarded With A Home Raid For Exposing E-Voting Vulnerabilities

Kavita Iyer

A programmer from Argentina who was trying to do a noble thing by uncovering critical vulnerabilities in the country's e-voting system was awarded for his good deeds with a police raid on his home.

Joaquín Sorianello told MSA, the company that manufactures the Vot.ar e-voting system, that the SSL certificates used by the system to encode transmissions between the central election office and voting stations could be downloaded without any difficultly, providing the opportunity for possible voting fraud (or just a good traditional DDOS attack).

Sorianello says that after informing the company regarding the flaw, he never received a phone call from MSA. However, he found out that his home was suddenly raided by Argentine police, who seized Kindles, computers and many storage devices (from a Google translation of the source):

> "*The truth is amazing, you notify the company that they have a failure in their voting system and the next thing they do is (raid my home) instead of looking for the real culprits…"I'm just a programmer, I'm not a hacker." Sorianello told La Nacion that he contacted the police station in Caballito to corroborate the raid: "They said yes, but they could not tell me why or how it was going to take." He also said he did not receive any call from the company (after having told them about the flaw a week) ago."*

Speaking to numerous news outlets, Sorianello has pointed out the fact that he is a programmer and not a hacker. He also said that had he desired to hack into the systems to cause damage to the company, he surely would not have given information to them of the flaw first. He also constantly pointed out that it was not him who published the important details of the e-voting internals but it was the protected @FraudeVotar Twitter account who had done it. Looks like that did not mean anything to the Argentinian legal system.

This is not the first issue that MSA and its e-voting technology, which is being used for the first time in Buenos Aires elections. The source code for the company's Vot.ar technology was leaked on GitHub two weeks ago. More recently, a group of researchers discovered a weakness in the system that they said could potentially allow a specially crafted e-voting ballot to be counted more than once. However, MSA said this would be almost very difficult to put in practice. Before you realize that this is all, in many cases, the technology Argentina is using just doesn't seem to work very well:

> "*Earlier today, the Argentinian site La Política Online reported that 532 polling stations were unable to transmit their results electronically to the central electoral office, and had to be transported there physically for the 184,000 votes involved to be included in the final result. As the article points out, although this failure won't change the outcome of the election for the head of local government in Buenos Aires, it will make a difference to the allocation of seats in the legislature and community boards."*

MSA's e-voting system is not only entirely open to several ways of fraud and attack, but it also works so pretty well that you need to physically transport the machines back to the central office to count the total number of votes.

In the mean time, Argentinian locals are stating that it was a good idea by the judge to give permission to the police to raid on Sorianello's house, who also ordered Argentina's National Authority for Information and Communication Technology to block many of the websites where information on the source code and e-voting flaws can be found.

For instance, justpaste.it has been ordered to block local access to five pages on its site that were related to the Buenos Aires elections. The details mentioned on those pages are still available elsewhere, which includes personal data about those involved in running the Buenos Aires polling stations as well as information of MSA's leaked SSL certificates. The official election site has some of this information is published on it, while other details such as mobile numbers and e-mail addresses are not, which may be why the judge ordered the pages to be blocked.

As we have noticed many other e-voting scandals of this type, you cannot run a safe and successful e-voting system without trust. And you surely cannot gain the public's trust by sending as many messages as possible and playing a pointless game with those who point out your system is absolutely and acutely flawed.

Source: Techdirt