Voter records for 80% of Chile's population left exposed online

Chile's Electoral Service confirms the data's authenticity, but denies it owns the leaky server.

By Catalin Cimpanu for Zero Day | August 1, 2019 -- 18:00 GMT (11:00 PDT) | Topic: Security

Santiago de Chile skyline

Image: Pablo García Saldaña

SEE ALSO

10 dangerous app vulnerabilities to watch out for (free PDF) (https://www.techrepublic.com/resource-library/whitepapers/10-dangerous-app-vulnerabilities-to-watch-out-for-free-pdf/?ftag=CMG-01-10aaa1b)

The voter information of more than 14.3 million Chileans, which accounts to nearly 80% of the country's entire population, was left exposed and leaking on the internet inside an Elasticsearch database.

ZDNet learned of the leaky server from a member of the Wizcase research team, who passed the server's IP to this reporter last week, in order to identify the nature and source of the leak.

We found that the database contained names, home addresses, gender, age, and tax ID numbers (RUT, or Rol Único Tributario) for 14,308,151 individuals.

Image: ZDNet

ZDNet has confirmed the validity and accuracy of this information with several of the individuals whose data was contained in the leaky database.

A spokesperson for Chile's Electoral Service -- Servicio Electoral de Chile (Servel) -- also confirmed the data's authenticity; however, they denied owning the leaky server.

VOTER RECORDS ARE FROM 2017

Both our private sources and the Servel spokesperson indicated that the data stored on the Elasticsearch server, hosted on the network of a US hosting provider, is at least two years old.

"The mentioned information corresponds to the data of 2017," a Servel spokesperson told ZDNet.

Inquired if the agency had allowed third-parties access to its data to build election-related apps, Servel said that "access to critical service data is not given to external contractors."

The agency said it's tasked by Chile's laws to keep the data up to date and provide an interface through which voters can verify the validity or update their voter information. This can be done via mobile apps or Servel's official website (https://consulta.servel.cl/).

Servel said it believes that there were people who scraped this information from its website and later assembled it in databases as the one ZDNet reported to the agency.

At the time of writing, the server is still online. The Wizcase team published their own report (https://www.wizcase.com/blog/chile-leak-research/) on the leaky server on their blog. WizCase researchers assessed that the server contained data "on nearly every Chilean adult," including high-profile politicians.

Data leaks: The most common sources (/pictures/data-leaks-the-most-common-sources/)

(/pictures/data-leaks-the-most-common-sources/6/)

(/pictures/data-leaks-the-most-common-

(/pictures/data-leaks-   (/pictures/data-leaks-   (/pictures/data-leaks-   (/pictures/data-leaks-   (/pictures/data-leaks-

MORE DATA BREACH COVERAGE:

- Robinhood admits to storing some passwords in cleartext (https://www.zdnet.com/article/robinhood-admits-to-storing-some-passwords-in-cleartext/)

- Hackers breach FSB contractor, expose Tor deanonymization project and more (https://www.zdnet.com/article/hackers-breach-fsb-contractor-expose-tor-deanonymization-project/)

- Bulgaria's hacked database is now available on hacking forums (https://www.zdnet.com/article/bulgarias-hacked-database-is-now-available-on-hacking-forums/)

- Credentials stuffing attack prompts password resets for Sky customers (https://www.zdnet.com/article/credentials-stuffing-attack-prompts-password-resets-for-sky-customers/)

- Slack resets passwords for 1% of its users because of 2015 hack (https://www.zdnet.com/article/slack-resets-passwords-for-1-of-its-users-because-of-2015-hack/)

- Thousands of Los Angeles police caught up in data breach (https://www.zdnet.com/article/thousands-of-los-angeles-police-caught-up-in-data-breach-personal-records-stolen/)

- A hacker assault left mobile carriers open to network shutdown (https://www.cnet.com/news/a-hacker-assault-left-mobile-carriers-open-to-network-shutdown/?ftag=CMG-01-10aaa1b) **CNET**

- 90% of data breaches in US occur in New York and California (https://www.techrepublic.com/article/report-new-york-california-hotbeds-for-data-breaches/?ftag=CMG-01-10aaa1b) **TechRepublic**

RELATED TOPICS: | SECURITY TV | DATA MANAGEMENT | CXO | DATA CENTERS

💬 SHOW COMMENTS