A leaky database of SMS text messages exposed password resets and two-factor codes

A security lapse has exposed a massive database containing tens of millions of text messages, including password reset links, two-factor codes, shipping notifications and more.

The exposed server belongs to Voxox (formerly Telcentris), a San Diego, Calif.-based communications company. The server wasn’t protected with a password, allowing anyone who knew where to look to peek in and snoop on a near-real-time stream of text messages.

For Sébastien Kaul, a Berlin-based security researcher, it didn’t take long to find.

Although Kaul found the exposed server on Shodan, a search engine for publicly available devices and databases, it was also attached to to one of Voxox’s own subdomains. Worse, the database running on Amazon’s Elasticsearch was configured with a Kibana front-end, making the data within easily readable, browsable and searchable for names, cell numbers and the contents of the text messages themselves.

Security updates for Friday

Google: Android Pie Updates Will Be A Lot Faster With Project Treble
Frustrating spammers [5]

Tracking and snooping on a million kids [6]

With a couple of watches paired to different testing phones, I had a play with various authorisation and Insecure Direct Object Reference, IDOR, attacks.

The only check the API appears to perform is matching the UID with the session_token, so simply changing the family_id in the get_watch_data_latest action, shown ibelow, allows an attacker to return the watch location and device_id associated with that family.

Security

Source URL: http://www.tuxmachines.org/node/117550

Links:
[3] https://lwn.net/Articles/772259/rss