Passwords For 540,000 Car Tracking Devices Leaked Online

Friday, September 22, 2017 Swati Khandelwal

Another day, another news about a data breach, though this is something disconcerting.

Login credentials of more than half a million records belonging to vehicle tracking device company SVR Tracking have leaked online, potentially exposing the personal data and vehicle details of drivers and businesses using its service.

Just two days ago, Viacom was found exposing the keys to its kingdom on an unsecured Amazon S3 server, and this data breach is yet another example of storing sensitive data on a misconfigured cloud server.

The Kromtech Security Center was first to discover a wide-open, public-facing misconfigured Amazon Web Server (AWS) S3 cloud storage bucket containing a cache belonging to SVR that was left publicly accessible for an unknown period.

Stands for Stolen Vehicle Records, the SVR Tracking service allows its customers to track their vehicles in real time by attaching a physical tracking device to vehicles in a discreet location, so their customers can monitor and recover them in case their vehicles are stolen.

The leaked cache contained details of roughly 540,000 SVR accounts, including email addresses and passwords, as well as users' vehicle data, like VIN (vehicle identification number), IMEI numbers of GPS devices.

Since the leaked passwords were stored using SHA-1, a 20-years-old weak cryptographic hash function that was designed by the US National Security Agency (NSA), which can be cracked with ease.

The leaked database also exposed 339 logs that contained photographs and data about vehicle status and maintenance records, along with a document with information on the 427 dealerships that use SVR's tracking services.

Interestingly, the exposed database also contained information where exactly in the car the physical tracking unit was hidden.

According to Kromtech, the total number of devices exposed "could be much larger given the fact that many of the resellers or clients had large numbers of devices for tracking."

Since SVR's car tracking device monitors a vehicle everywhere for the past 120 days, anyone with access to SVR users' login credentials could both track a vehicle in real time and create a detailed log of every location the vehicle has visited using any internet connected device like a desktop, laptop, mobile phone or tablet.

Eventually, the attacker could outright steal the vehicle or even rob a home when they know a car's owner is out.

Kromtech responsible alerted the company of the misconfigured AWS S3 cloud storage bucket, which has since been secured. However, It is unclear whether the publically accessible data was possibly accessed by hackers or not.

Swati Khandelwal
Technical Writer, Security Blogger and IT Analyst. She is a Technology Enthusiast with a keen eye on the Cyberspace and other tech related developments.