**Nissan LEAF vulnerability provides an extremely easy way for anyone to control heating system and get driving history**

As per the [report](http://www.troyhunt.com/2016/02/controlling-vehicle-features-of-nissan.html) by the security developer/researcher Troy Hunt, Nissan’s LEAF, the [world’s best selling electric car](http://www.greencarreports.com/news/1096118_nissan-leaf-sets-new-annual-record-for-u-s-electric-car-sales), has a vulnerability that provides an extremely easy way for anyone to control any LEAF’s heating system and get the driving history.

Nissan LEAF has a companion [app](https://itunes.apple.com/ca/app/nissan-canada-leaf/id450031231?mt=8) that allows users to control the car’s heating system and get their driving history, among other things. Nissan appears to use some RESTful APIs to provide these services. As Troy Hunt demonstrates in this [video](https://www.youtube.com/watch?v=Nt33m7G_42Q), these APIs require no form of authentication whatsoever; anyone with any web browser/HTTP client can start messing around with any LEAF’s heating system and get their driving history. This is because the only form of “authentication” used by the APIs is the car’s VIN number that is provided as part of the request URL. But except for the last five digits, the VINs for all the LEAFs are exactly identical! So, one can literally iterate over all these VINs pretty quickly. If the car has been registered on the Nissan’s servers (i.e., the owner is using the app), and you’re using the correct root URLs (the app uses different domains based on location, but with the same APIs), then the APIs will just give anyone the data. Besides, each unit’s own VIN is written on the outside of the vehicle (stencilled on the windscreens), and is thus easily locatable. So getting the information for a specific LEAF is even easier.

Although, this vulnerability is not as severe as, say, compromising the car’s steering system, it can have its own consequences. Nissan has safeguards in place that doesn’t allow someone to change the heating systems via the app while driving, but when parked, someone can turn these on and deplete the battery, potentially stranding the person in dangerous situations. This is extremely serious considering the popularity of this vehicle in Europe, Canada, and Australia, all of which have their own versions of extreme weathers/regions. Besides, access to someone’s driving history can allow someone to deduce their daily schedules, potentially leading to actual burglaries, as I explained in a [previous article](https://eclass.srv.ualberta.ca/mod/forum/discuss.php?d=601522&parent=1578083) with the example of thermostat data.

According to the [BBC report](http://www.bbc.com/news/technology-35660641), and deducing by the angry comments on the app’s review page, Nissan has temporarily shut down the online service. Nissan assures the owners that “no other critical driving elements of the Nissan Leaf or eNV200 are affected, and our 200,000-plus LEAF and eNV200 drivers across the world can continue to use their cars safely and with total confidence”; the electric van nNV200 is also affected by the shutdown of the online service. So, it appears that Nissan has taken the situation under control without much reported damage, but it is yet another example of how not prioritizing the security of the IoT devices can lead to pretty serious (and almost humorous) flaws.