“Optusdata” told Information Security Media Group reporter Jeremy Kirk they had acquired the data through an unsecured Application Programming Interface (API), which allowed access to Optus’s customer database from devices anywhere on the public internet.

The hacker was able to access the information of all of the company’s customers by running an automated script that asked for database records one-by-one, simply increasing the “contactId” index number by one with each request.

“Optusdata” explained that no username, password or authentication token was required, writing to Kirk: “No authenticate needed. That is bad access control. All open to internet for any one to use.”

APIs are used extensively to allow communication between different pieces of software, within a single device or across networks. When Optus customers view their account via a mobile app or the web, a similar API to the one that was breached is used to retrieve and display their own information. Properly implemented, this is only possible after logging in, and cannot be used to display the details of other customers.

Security experts have speculated that the exploited API was a new version that was being tested and was not intended to be accessible from the public internet. To protect security, such an API should have used test data rather than actual customer details.

Kirk’s analysis of public Domain Name System (DNS) records—essentially the internet equivalent of a phone book—suggests that the unsecured API may have been accessible for up to three months.

The massive breach points to the danger of placing sensitive data in the hands of vast corporations, whose only concern is profit. While the Optus data breach is notable for its vast scale, hacks accessing substantial amounts of personal data are increasingly common.