The Optus data breach occurred through an unprotected and publically exposed API. This API didn’t require user authentication before facilitating a connection. A lack of an authentication policy meant anyone that discovered the API on the internet could connect to it without submitting a username or password.

Security Flaw #1

Three security flaws can be identified in this setup. The first is a public-facing API (Application Programming Interface. An API should never be public-facing if it facilitates access to sensitive internal data or permits interactions with core business operations. Examples of open APIs that follow best API security practices are the Google Maps API and the Weather API. Any data that's available through these APIs is completely isolated from core business processes, so it’s impossible to cause a data breach through these open APIs.

*Is your organization at risk of a data breach?*[*Click here to find out*](https://www.upguard.com/instant-security-score)*.*

Security Flaw #2

This brings us to Optus’ second security flaw. The open API facilitated access to very sensitive customer data. To get a sense of the level of sensitive data this API was granting access to, whenever an Optus customer loads their account information either via the Optus mobile app or the Optus website, an API such as the one that facilitated the data breach is used to complete the request.

Backend processes call upon sensitive customer records to load a customer profile. This is why the Optus data breach resulted in the compromise of the following types of personal data:

* Driver’s License numbers
* Phone numbers
* Dates of birth
* Home addresses

[According to an analysis](https://www.wsws.org/en/articles/2022/10/06/afrq-o06.html) of public Domain Name System (DNS) records by security analyst Jeremy Kirk, this unsecured API was likely public-facing and, therefore, accessible to anyone on the internet for up to three months.  
‍

[[](https://www.upguard.com/security-report/optus)](https://www.upguard.com/security-report/optus" \t "_blank)

See how your organization's security posture compares to Optus'.

[View Optus' security report.](https://www.upguard.com/security-report/optus)

‍

Security Flaw #3

The third and final security flaw in this vulnerability package was the use of incrementing customer identifiers. In the digital world, programs identify customers by a unique sequence of numbers and letters. These are the identifiers that are called upon when a customer loads their account. According to best cybersecurity practices, each customer identifier, or contactID, should be completely unique and unrelated to other identifiers to prevent hackers from discovering the formula that determines each customer ID.

In Optus’s case, all customer identifiers differed by an increment of 1. So if one customer had the unique identifier 5567, the next customer in the database could be found with the identifier 5568.

When a hacker gains access to a customer database, the first thing they do is cross their fingers and check whether data identifiers increase incrementally. If this is the case, brute force techniques aren’t necessary, and the process of stealing data becomes much easier.

When the hacker responsible for the Optus breach gained access to the company’s customer database, they were very pleased to find that all customer records were indeed stored with incrementing identifiers. This allowed them to write a script that requested every customer record in the database by simply incrementing each contactID index by one.

With virtually the entire data exfiltration process outsourced to an automated script, the hacker was able to complete the data breach much faster and at a much larger scale than it would have other been possible if unique customer identifiers had been used.

With virtually the entire data exfiltration process outsourced to an automated script, the data breach was completed much faster and at a much larger scale. This unfortunate efficiency led to the Optus breach becoming ranked as the second-largest data breach in Australian history.

During the entire period these three vulnerabilities were active - which is likely to be three months - 9.8 million Optus customers were always at risk of compromise through a domino effect of mounting exploitation severity. All that was required to initiate the breach was for a cybercriminal to eventually discover this perfect domino stack, and give it just one gentle push