Articles used as part of the research:

<https://www.cshub.com/attacks/news/iotw-everything-we-know-about-the-optus-data-breach>

<https://thehackernews.com/2022/10/19-year-old-hacker-arrested-for-using.html>

<https://www.reuters.com/technology/australia-unveils-privacy-rule-changes-after-optus-data-breach-2022-10-06/>

<https://www.bleepingcomputer.com/news/security/optus-confirms-21-million-id-numbers-exposed-in-data-breach/>

<https://securityboulevard.com/2022/10/optus-data-breach-why-vulnerable-apis-are-to-blame/>

<https://www.cshub.com/attacks/news/iotw-everything-we-know-about-the-optus-data-breach>

Optus Breach Analysis

Optus, a Singapore Telecommunications Ltd-owned business, had up to 10 million records stolen in a breach that was initially detected on September 22. Optus claims that as soon as the breach was detected, they contained and removed access from the attackers. Following the discovery on the 22nd of September, the attacker, under the name optusdata, posted a ransom request on Breached. This post contained around 10,000 records as evidence that they had compromised Optus. On the 27th, optusdata deleted their previous post with the excerpt of data.

To date, not much has been released on how the breach happened or the root cause. This is not uncommon for large organizations. It likely will take even longer to fully understand the incident, due to the total amount of records exposed, as it makes the investigation even more tedious. However, based on an article published by [Security Boulevard](https://securityboulevard.com/2022/10/optus-data-breach-why-vulnerable-apis-are-to-blame/) on October 3rd, it appears that the data was extracted through an exposed API. To make this worse, it is being reported that the API was exposed accidentally for a test environment that had access to production-quality data without proper authentication applied. In short, this breach could have been conducted by a script kiddie that found the API and proceeded to use readily available tools to query API endpoints.

If this reporting rings true in the coming weeks, this may very well force some additional changes in regulation that have already been proposed. As reported by [Reuters](https://www.reuters.com/technology/australia-unveils-privacy-rule-changes-after-optus-data-breach-2022-10-06/) and many other outlets, there are already proposed changes to consumer privacy regulations in Australia. In fact, additional regulations and laws may be passed sooner than later. It is being reported that a 19 year old was arrested on October 6th, after attempting to conduct an SMS-based extortion campaign against the 10,000 records that were exposed by optusdata in early September ([The Hacker News](https://thehackernews.com/2022/10/19-year-old-hacker-arrested-for-using.html)). This has placed additional pressure on government officials, Optus, and banks in Australia to protect those who had their data stolen as part of this breach. In fact, the Australian government is already pushing to create a fraud database that is made up of those individuals that had their data stolen for financial institutions to use to help with detecting fraud or identity theft.

Beyond the initial knee-jerk reaction and conjecture that many politicians and security practitioners are making, there will be a slow trickle of response to this breach going forward. Unfortunately, now that the data is out there and pending the reporting of optusdata deleting the trove of information being false, there is no way for these individuals to secure their data again or get it back into trusted hands. Going forward, all these individuals who had their data compromised can do is to monitor their credit and identity going forward to try to detect any identity fraud that may happen. There may be some regulations or changes in always to try to address this, but it will not make any material change to the events that have already passed. We, as a technology industry, can only try to learn from this event and better secure data in the future.