Reports suggest Optus had an application programming interface (API) available online that did not require authorisation or authentication to access customer data.

“In the instance, where a public API endpoint did not require authentication, anyone on the internet with knowledge of that endpoint [URL] could use it,” said senior manager of cyber security consulting for Moss Adams, Corey J Ball.

“If that endpoint was used to access customer data, then anyone on the internet could have used that endpoint to gather customer data.

“Without technical controls for authentication and authorisation in place, any user could have requested any other user’s information. The attacker likely scripted the process to repeat requests from the endpoint until they had collected millions of instances of personally identifiable information.

Optus still hasn’t confirmed how the data was accessed. It maintains the attack was sophisticated, but the home affairs minister, Claire O’Neil, has said the vulnerability was akin to Optus leaving a window open.