Australian Government
Office of the Australian Information Commissioner

Medibank data breach: alleged timeline

This infographic summarises the Australian Information Commissioner's alleged timeline of the Medibank data breach as set out in the concise statement filed in the Federal Court.

Before 7 August 2022

An employee of a third-party IT provider contracted by Medibank saved their Medibank credentials to their personal internet browser profile on their work computer. These credentials were then synced to their personal device. This person had a Medibank admin account.

Around 7 August 2022

The Medibank credentials were stolen from the third-party's employee's personal device by malware.

12 August 2022

The threat actor tested the Medibank credentials for the admin account.

Around 23 August 2022

The threat actor authenticated and logged onto Medibank's virtual private network (VPN), which allowed remote access to the Medibank corporate network. They installed a malicious script.

At the time, Medibank's VPN did not require 2 or more proofs of identity or multi-factor authentication; only a device certificate or a username and password was required.

Around 24–25 August 2022

Medibank's endpoint detection and response (EDR) security software generated various alerts that were sent to the Medibank IT Security Operations email inbox, but not appropriately triaged or escalated at the time.

Around 25 August–13 October 2022

The threat actor accessed numerous Medibank systems and extracted approximately 520GB of data. The EDR software generated further alerts, which were not appropriately triaged or escalated at the time.

11 October 2022

Medibank's IT Security Operations team triaged a high severity incident after an alert and engaged a third party to investigate.

Around 16 October 2022

The third party noticed suspicious volumes of data had been extracted.

19 and 22 October 2022

The threat actor contacted Medibank and provided sample data as evidence of the breach.

9 November–1 December 2022

The threat actor published data on the dark web.

OAIC