SALT

TOP 10 API Data Breaches

LinkedIn (2021)
700m users impacted

LinkedIn's API was exploited to scrape user data such as email addresses, phone numbers, and professional details which were sold on the dark web.

Facebook (2019)
533m users affected

An API vulnerability exposed phone numbers linked to user accounts. Hackers used this flaw to scrape user data leading to leakage and investigations.

Dell (2024)
49m records impacted

Exposed a significant amount of customer information, including names, addresses, order details, and service tags, due to a vulnerability in Dell's partner portal.

T-Mobile (2023)
40m users affected

A misconfigured API allowed hackers to access personal data, Social Security numbers and driver's license information, costing the company huge compensation costs.

Panera Bread (2018)
37m customers impacted

An API vulnerability exposed customer records, including email addresses and partial credit card information.

Optus (2022)
10m accounts affected

An unauthenticated API endpoint exposed sensitive customer information, including ID numbers and addresses leading to further extortion attempts.

Twitter (2022)
5.4m accounts impacted

A vulnerability in Twitter's API allowed hackers to link email addresses and phone numbers to Twitter profiles. User data was sold on the dark web.

Snapchat (2014)
4.6m accounts impacted

API security weaknesses allowed hackers to expose user data like phone numbers and usernames. This data was later leaked online.

GitHub (2020)
50k+ API keys and secrets leaked

Sensitive credentials were exposed, allowing potential access to private databases and systems.

Duolingo (2023)
2.6m users impacted

A vulnerable API allowed data scraping, exposing user information like email addresses and usernames. User data was then sold on hacking forums.