CEQUENCE

FRIGHTENING API FAILURES

The Spookiest Breaches of 2024

2024 was filled with some memorable breaches, but none more consistently scary than API breaches and bot attacks. Here is a summary of the worst breaches in the last 6 months. Scroll to the end to find out how to protect your APIs from the next terrifying attack!

LIFE360

442,519 IMPACTED

A threat actor leaked a database containing the personal information of 442,519 Life360 customers collected by abusing a flaw in the login API.

TRELLO

15,000,000 IMPACTED

Hacker gained access through an API endpoint that could be accessed without logging in, to allow software to work together in distributed systems. This API allows developers to search for public information about a profile based on users' Trello IDs, usernames, or email addresses.

RABBIT

UNKNOWN NUMBER IMPACTED

A group of developers and researchers called Rabbitude says it discovered API keys hardcoded in the company's codebase, putting sensitive information at risk of falling into the wrong hands.

TWILIO

UNKNOWN NUMBER IMPACTED

An unsecured API endpoint allowed threat actors to verify the phone numbers of millions of Authy multi-factor authentication users, potentially making them vulnerable to SMS phishing and SIM swapping attacks.

DROPBOX

UNKNOWN NUMBER IMPACTED

A threat actor accessed data from Dropbox Sign's API keys, OAuth tokens, and multifactor authentication (MFA) details. This is all data used by third-party partners to connect to the service and offer seamless integration from their respective online services, with OAuth in particular being weaponized by threat actors.

GITHUB

12,800,000 IMPACTED

GitHub users accidentally exposed 12.8 million authentication and sensitive secrets in over 3 million public repositories during 2023, with the vast majority remaining valid after five days.

TICKETMASTER

560,000,000 IMPACTED

Hackers hawked stolen info of 560M users. The incident comes as Ticketmaster faces increased scrutiny from federal investigators over its business practices and its inability to stop bot farms that buy tickets almost instantaneously and allow people to upsell them.

DROPBOX

UNKNOWN NUMBER IMPACTED

A threat actor accessed data from Dropbox Sign's API keys, OAuth tokens, and multifactor authentication (MFA) details. This is all data used by third-party partners to connect to the service and offer seamless integration from their respective online services, with OAuth in particular being weaponized by threat actors.

DELL

49,000,000 IMPACTED

The threat actor behind the recent Dell data breach revealed they scraped information of 49 million customer records using an partner portal API they accessed as a fake company.

QUANTAS

UNKNOWN NUMBER IMPACTED

Ted Miracco, CEO of mobile application security specialist Approov, said that as such, the incident was highly concerning. "The problem described suggests a significant issue with how user sessions and data are being handled within the app," he said. "The application programming interface (API) is incorrectly processing or validating session tokens, leading to unauthorised access to data.

PANDABUY

1,300,000 IMPACTED

PandaBuy data was stolen by exploiting several critical vulnerabilities in the platform's API and other bugs were identified allowing access to the internal service of the website," the hackers posted.

To mitigate risks like these, businesses should consider these steps:

1 Conduct Regular Security Assessments

Perform vulnerability assessments and penetration testing on your APIs and applications to identify and address potential weaknesses.

2 Implement Strong Authentication Mechanisms

Use multi-factor authentication (MFA) and OAuth 2.0 to secure access to APIs, ensuring only authorized users and applications can interact with your systems.

3 Maintain an Up-to-Date Inventory

Keep a detailed inventory of all public-facing applications and APIs. Regularly review and update this list to avoid vulnerabilities from overlooked endpoints.

4 Monitor and Analyze User Behavior

Continuously monitor user activity for unusual patterns, such as sudden spikes in logins or access from unfamiliar IP addresses, to detect potential account takeovers or bot attacks.

5 Utilize Threat Intelligence

Incorporate threat intelligence to stay informed about emerging threats and adapt accordingly.

6 Enforce Rate Limiting and Throttling

Implement rate limiting to control the number of requests a user or application can make to your APIs, reducing the risk of abuse and DDoS attacks.

Visit www.cequence.ai/assessment/ to find out if a serious API vulnerability could turn into a nightmare for your organization.

CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai