Security Data Breach

Twitter

Security Data Breach (2022)

On January 4, 2023, Twitter, one of the largest social media organizations, learned that bad actors were responsible for the data breach. The summary of the incident is as follows:

- Over 200 million Twitter accounts were allegedly leaked by hackers. This result came from approximately 400 million sets from the database, including duplicates;
- Their information was published on a popular hacker forum for about $2;
- Twitter database was exploited by API;
- Even though this type of leak was fixed on January 2022, more and more data-leaking actors leak data sets.

Company Background

- Twitter is a social media organization found in March 21, 2006. It is based in San Francisco, California and has more than 25 offices around the world.
- Between the year 2010 and the year 2020, the number of Twitter users was booming from 100 million to more than 330 million, where it is known that "approximately 48 million accounts were fake".
- Elon Musk, the founder and CEO of SpaceX, gained control over Twitter as the CEO on October 27, 2022, where more than 4,000 staffs were laid off. He announced he would step down as the CEO once a replacement had been found.
- Similar instances continue, including:
  - Hacker posted 5.4 million users for sale (July 2022);
  - Former employee was found guilty of spying for Saudi Arabia (August 2022);
  - Hacker published data on 5.4 million users (November 2022)

Timeline

Twitter Data Breach

1. **January 2022:** The vulnerability, following the data breach, was first identified and dealt.
2. **July 21, 2022:** A hacker under the alias 'devil' posted on *BreachForums* that they had obtained from a dataset of 5.4 million users.
3. **August 2022:** A federal jury in California found the Twitter employee guilty for acting as an unregistered agent for the government in Saudi Arabia.
4. **November 24, 2022:** Personal information of approximately 5.4 million Twitter accounts were leaked on a hacker forum, following the exploitation of API vulnerability.
5. **January 4, 2023:** Over 200 million Twitter accounts were leaked in a hacker forum for $2. High-profile accounts, including Donald Trump Jr, were leaked. The suspect is a hacker different from the one in November 2022.
6. A threat actor named "Ryushi" attempted to ransom the data of over 400 million "for an exclusive sale".

Vulnerabilities

The information on the right displays most recent vulnerabilities recorded since the year 2020. Top two right vulnerabilities are associated with the 2022-2023 data breach, whereas bottom two are vulnerabilities detected by Twitter.

API Exploitation

Allowed a bad actor to find out the account names associated with certain email addresses and phone numbers. A hacker was able to exploit the flaw before Twitter noticed it.

Security Vulnerability

Twitter confirmed on Wednesday (January 11, 2023) that the "bug bounty program" was patched in January 2022.

Injection Vulnerability

According to CVE Details, an injectivity vulnerability is present in previous versions since 2019, following application errors. The availability impact was partial, and there was no confidentiality impact.

Certificate Exploitation

The Twitter Kit framework does not properly validate the SSL certificate, coming from implementation issues. That include "a lack of hostname verification." There were partial confidentiality impact, concerning the informational disclosure.

Costs

- A "devil" actor imposed the sale on a breached data forum database of phone numbers and email addresses belonging to 5.4 million accounts. The price was set to $30,000.
- Security breach vulnerability affected Android users and allow anyone without authentication to access to an account by phone submission.
- Data-breach costs in 2021 were estimated to have risen to $4.24 million from $3.86 million in 2020, according to the latest annual study from US technology company IBM.
- Risk of paying hundred millions of US dollars in GDPR breach fines

Prevention

As Twitter has no further communications or updates on advanced solutions for preventing further breaches, most recent prevention methods include:

- On January 13, 2022, Twitter fixed the flaw disclosed, following the incident on January 1, 2022.
- Twitter recommends not to include phone number or email address.
- Two-factor authentication (2FA) is encouraged, whether in the form of apps or hardware keys.