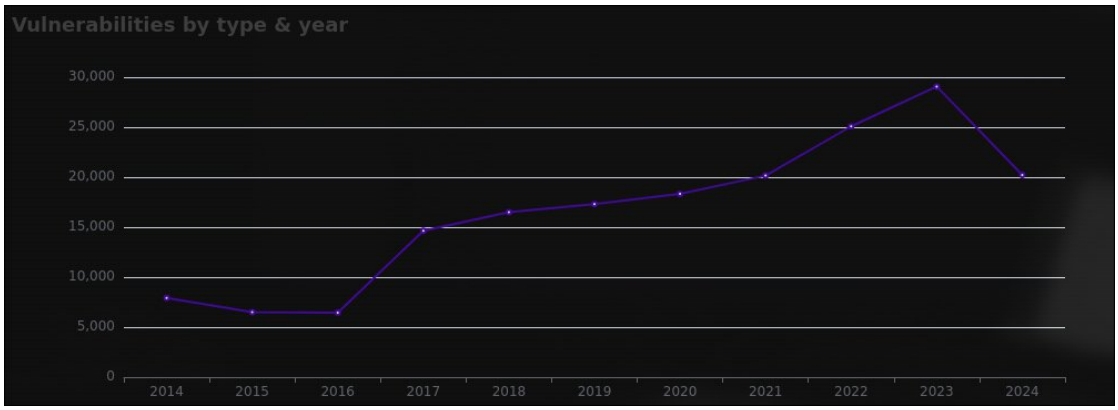
Vulnerabilities over the Years



Analysis of Cyber Attack Vulnerabilities from 2014 to 2024

We have a graph that shows the number of cyber attack vulnerabilities each year from 2014 to 2024. Let's look at what happened in each period and try to understand why, with real-life events included.

1. Between 2014 and 2016

- **Steady Numbers**: From 2014 to 2016, the number of vulnerabilities stayed between 5,000 and 10,000. This means that not many new weaknesses in computer systems were being found and reported.
- **Relevance**: During this period, cybersecurity was important, but there wasn't a huge focus on it. Companies were still using older systems and detection tools, so not many vulnerabilities were discovered.

2. Big Jump in 2017

- **Why the Big Jump?** In 2017, the number of vulnerabilities jumped up a lot. Here are some possible reasons:
- **Better Tools**: Companies started using better tools to find weaknesses in their systems.

- **Major Cyber Attacks**:
- **WannaCry Ransomware Attack (May 2017)**: This was a massive cyber attack that affected computers worldwide. It made people realize how important it was to find and fix vulnerabilities.

- **Equifax Data Breach (September 2017)**: Personal data of 147 million people was exposed. This breach showed the importance of cybersecurity.

- **New Rules**:
- **General Data Protection Regulation (GDPR)**: Although it came into effect in 2018, preparations for GDPR made companies more focused on finding and reporting vulnerabilities to avoid huge fines.

3. Gradual Increase Till 2021

- **Why the Increase?** From 2017 to 2021, the number of vulnerabilities kept increasing but at a normal pace. This can be because:
- **Improved Detection**: Security experts got better at finding vulnerabilities.
- **More Awareness**: More companies started looking for vulnerabilities because they became more aware of cyber threats.
- **Relevance**: Events like the continuous revelations of data breaches (e.g., Yahoo's disclosure of additional breaches in 2017) kept

cybersecurity in the spotlight. Companies were investing more in cybersecurity to protect themselves.

4. Peak in 2023

- **Why the Peak?** In 2023, the number of vulnerabilities reached the highest point. Possible reasons include:
- **COVID-19 Impact**: The pandemic (starting in 2020) forced a lot of people to work from home and use online services more, which might have exposed more vulnerabilities.

- **Remote Work Surge**: With more people working from home, the use of personal devices and home networks increased, leading to more security challenges.

- **More Cybercrime**: Hackers were very active, taking advantage of the situation.
- **Relevance**: Increased cybercrime activities during the pandemic, such as phishing attacks targeting remote workers, highlighted more vulnerabilities.
- **Better Reporting**: With better tools and more experts, more vulnerabilities were being found and reported.

5. Drop in 2024

- **Why the Drop?** In 2024, the number of vulnerabilities went down. Here are some reasons why this might have happened:
- **Better Security**: Companies might have improved their security measures, making it harder to find new vulnerabilities.

- **Relevance**: Investments in cybersecurity post-pandemic, including better security technologies and more robust security practices, could have reduced the number of new vulnerabilities.
- **Advanced Tools**: The tools for finding vulnerabilities might have become so good that fewer new ones were being discovered.
- **Incomplete Data**: It could also be that the data for 2024 isn't complete yet, so the final number might be higher later.

Conclusion

The graph shows that the number of cyber attack vulnerabilities has changed a lot over the years. From 2014 to 2016, the numbers were steady, but there was a big jump in 2017 due to better tools and major cyber attacks like WannaCry and the Equifax breach. The numbers kept increasing till 2021 because of improved detection and more awareness. In 2023, the number of vulnerabilities peaked, possibly due to the effects of the pandemic and more cybercrime. Finally, the drop in 2024 might be because of better security or incomplete data.

Understanding these trends helps us know how important it is to keep improving our cybersecurity measures to protect against cyber attacks.