Химач Д.С.,
учень 11-Б класу Наукового ліцею Житомирської політехніки
Науковий керівник: Шатківський В.М.,
вчитель інформатики,
Відокремленого підрозділу "Науковий ліцей"
Державного університету "Житомирська політехніка"
pzs_shvm@ztu.edu.ua

АНАЛІЗ БАЗИ ДАНИХ CVE

У сучасних умовах, коли інформаційні технології стали невід'ємною частиною всіх аспектів нашого життя, безпека цифрових ресурсів набуває особливого значення. Останніми роками загроза кіберзлочинності значно зросла, і зокрема, це посилилося в умовах повномасштабного вторгнення рф на територію України, від чого збільшилася діяльність кібершахраїв і хакерських груп. Аналіз переліків відомих вразливостей є важливим процесом для забезпечення безпеки вебсайтів та захисту конфіденційних даних. Вчасне виявлення та усунення уразливостей дозволяє знизити ризики несанкціонованого доступу, збереження даних та безпеки користувачів.

На даний момент існують наступні системи для ідентифікації та класифікації вразливостей:

- ➔ CWE (Common Weakness Enumeration), яка описує програмні слабкості
- ➔ Exploit-DB, яка містить вразливості та відповідні експлойти
- ➔ NVD (National Vulnerability Database), що надає додаткові метадані до CVE
- ➔ OSVDB(Open Source Vulnerability Database), орієнтована на вразливості в програмному забезпеченні з відкритим кодом
- ➔ SecurityFocus, що надає інформацію через базу даних Bugtraq
- ➔ CVE (Common Vulnerabilities and Exposures) — це каталог відомих проблем у програмному забезпеченні, які можуть становити небезпеку для користувачів.

Кожна система має свої переваги, залежно від сфери використання та специфіки програмного забезпечення.

Варто відзначити, що CVE забезпечує стандартизацію ідентифікації вразливостей, надаючи кожній з них унікальний номер у форматі CVE-рік-порядковий номер, наприклад, CVE-2024-12345. Цей формат дозволяє легко відслідковувати вразливості за роком виявлення, що допомагає уникнути плутанини, яка може виникати через різні назви для однієї й тієї ж вразливості в різних базах даних. Завдяки цьому CVE є основою для багатьох інструментів кібербезпеки і використовується як загальноприйнятий стандарт у світовій спільноті. Це полегшує обмін інформацією між організаціями та дає можливість легко порівнювати й аналізувати дані про вразливості в різних системах та продуктах.[1]

Для оцінки критичності кожної вразливості зі списку бази даних CVE використовується CVSS (Common Vulnerability Scoring System) — стандартизована система оцінки, яка призначає кожній вразливості числовий бал, що характеризує її небезпеку. CVSS дозволяє фахівцям з кібербезпеки отримати швидке уявлення про рівень ризику, який становить конкретна вразливість, відображаючи її потенційний вплив на інформаційні системи, дані або мережі.

Система CVSS використовує шкалу від 0 до 10, де вищі бали вказують на більшу критичність вразливості. Оцінка розраховується на основі кількох ключових факторів, таких як легкість експлуатації вразливості, можливий збиток, який вона може завдати, а також наявність доступних методів захисту. Завдяки CVSS фахівці з кібербезпеки можуть ефективно пріоритизувати виправлення вразливостей, концентруючи ресурси на усуненні найбільш критичних загроз. Це забезпечує своєчасне усунення вразливостей, що мають найвищий ризик, і підвищує загальний рівень захисту систем від потенційних атак.[2]

В умовах сучасних кібер-ризиків, особливо посилених зростанням активності хакерських груп і кібершахраїв, стандартизовані підходи до оцінки ризиків, такі як CVE, допомагають фахівцям з кібербезпеки не лише своєчасно виявляти вразливості, а й раціонально використовувати ресурси для усунення найбільш критичних загроз. Усе це робить CVE незамінним елементом з кібербезпеки, підвищуючи захист інформаційних систем тапокращує безпеку користувачів.

Список використаних джерел:

1. What is a CVE? URL: https://www.redhat.com/en/topics/security/what-is-cve
2. What is Common Vulnerability Scoring System (CVSS Score). URL: https://www.sans.org/blog/what-is-cvss/