Толокнов Анатолій Арнольдович

Національний університет «Одеська юридична академія»,

асистент кафедри інформаційних технологій

ОГЛЯД БАЗ ДАНИХ ВРАЗЛИВОСТЕЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Під вразливістю інформаційної системи розуміють таку властивість системи, з якої можлива реалізація загрози її безпеки [1]. Оцінивши ризики та ймовірність певних загроз, можна вибрати, яка вразливість є більш прийнятною з точки зору ймовірності реалізації дочірніх загроз та величини отриманих від них збитків. Не існує інформаційних систем, що не містять вразливостей, існують лише настільки захищені, стосовно яких можна сказати, що ймовірність виникнення актуальних загроз безпеці інформації є прийнятною.

У 90-ті роки XX століття, у зв'язку з розвитком Інтернету, стала очевидною необхідність систематичного збору даних про вразливості програмного забезпечення (ПЗ) та їх каталогізації. Актуальність цього завдання була зумовлена і появою нових видів ПЗ: операційних систем та серверних платформ, прикладних програм, веб-застосунків та ПЗ для вбудованих систем, збільшенням числа версій у лінійці одного і того ж програмного продукту, а також зростанням частоти виявлення в цих програмах вразливостей, що дозволяє зловмиснику отримати повний контроль над комп'ютерною системою або доступом до критичної інформації.

Створення реєстрів та баз даних з інформацією про виявлені вразливості потребувало уніфікованого способу їх ідентифікації та класифікації. Дані про індивідуальні вразливості в сукупності з організованим зберіганням, функціями пошуку по базі та автоматичного отримання повідомлень про нові виявленні вразливості можуть бути корисні широкому колу фахівців у галузі інформаційної безпеки. Кінець 90-х і початок 2000-х років характеризувався появою цілого ряду каталогів і баз даних вразливостей, підтримкою яких займалися різні, незалежні один від одного, організації. Поява та розвиток незалежних однієї від одної баз

даних та реєстрів вразливостей породило проблему синхронізації інформації між ними.

Стандарт Common Vulnerabilities and Exposures (CVE), розроблений американською некомерційною дослідницькою корпорацією MITRE Corporation у 1999 році [2], де-факто є на сьогоднішній день основним стандартом у галузі уніфікованого найменування та реєстрації виявлених вразливостей програмного забезпечення.

Основними задачами організацій, що входять в проект MITRE CVE, є:

- пошук та збір інформації про вразливість програмного забезпечення;
- класифікація знайдених вразливостей;
- резервування CVE-ідентифікаторів для знайдених вразливостей;
- оновлення відповідної інформації в двох офіційних каталогах – реєстр вразливостей CVE List (https://cve.mitre.org/cve/) самої корпорації MITRE і бази даних вразливостей NVD (National Vulnerability Database, https://nvd.nist.gov/) , підтримується національним Інститутом Технології та Стандартів США.

На сьогоднішній день бази вразливостей MITRE CVE List і NVD містять близько 98 тисяч записів про окремі вразливості, виявлені за період з 1999 року до теперішнього часу. Ідентифікатори CVE мають формат CVE-YYYY-NNNN, відображають в перших чотирьох цифрах рік реєстрації вразливості та в наступних чотирьох-шістьох цифрах – унікальний номер вразливості у рамках цього року.

База VND (Vulnerability Notes Database) підтримується центром реагування CERT/CC при Інституті програмної інженерії в університеті Карнегі-Меллона, США [3].

Кожен запис у базі VND агрегує інформацію про безліч подібних вразливостей для будь-якого конкретного ПЗ, посилаючись на множину відповідних CVE ідентифікаторів. Дана агрегація є характерною відмінністю бази VND від баз CVE List і NVD, дозволяючи перевірити безліч вразливостей подібної природи в конкретному вразливому ПЗ або його компоненті.

Крім цього, записи в базі VND часто містять докладний і детальний посібник з усунення вразливостей та/або запобігання їх експлуатації

зловмисником, а також огляд поточної ситуації з наявністю або успішним закриттям виявленої вразливості різними вендорами.

Дані характеристики бази VND належать до її сильних сторін і доповнюються дозволом на безкоштовне використання всіх матеріалів бази для будь-яких цілей і можливістю повного завантаження всіх записів бази у форматі JSON за допомогою спеціального програмного забезпечення, що безкоштовно надається.

Альтернативним підходом до каталогізації інформації про виявлені вразливості ПЗ є реєстрація не самих вразливостей, а сценаріїв їх експлуатації (експлойтів, exploits) або прикладів експлуатації вразливості (Proof of Concept). Прикладом реалізації такого підходу є база Exploit Database [4], сформована організацією Offensive Security Team, що спеціалізується на проведенні тренінгів з інформаційної безпеки та тестування комп'ютерних систем на проникнення.

База Exploit Database на даний момент містить близько 44,5 тисяч записів, розбитих на різні категорії (експлойти для веб-застосунків, віддаленої та локальної експлуатації вразливостей, приклади атак Denial of Service та можливі фрагменти коду shellcode для різних вразливостей переповнення стека або доступу до пам'яті). Дані записи покривають безліч вразливостей, виявлених з 2000 року до теперішнього часу.

Типовий запис у базі Exploit Database містить короткий опис вразливості, вказівку вразливих версій додатків або їх компонентів, вразливу програмну платформу (операційну систему або фреймворк веб-застосунку), CVE-ідентифікатор, присвоєний даній вразливості (за його наявності). Однак найважливіша і змістовна частина запису – це детальний опис причин виникнення вразливості, місця локалізації вразливості в коді (з безпосередньою демонстрацією вразливого фрагмента коду, якщо код програми публічно доступний) і опис працездатних сценаріїв експлуатації вразливостей або сценаріїв Proof of Concept.

Різноманітність різних реєстрів та баз даних вразливостей викликає у фахівців у галузі інформаційної безпеки бажання використовувати різного роду агрегатори інформації, які б забезпечували автоматизований збір доступної

інформації про вразливості та додаткові функції пошуку та фільтрації інформації.

Прикладом такого сервісу є CVEDetails (https://www.cvedetails.com/) – простий спеціалізований агрегатор інформації про вразливості, який збирає всю доступну з публічних реєстрів та баз даних вразливостей інформацію щодо конкретного CVE-ідентифікатора та об'єднує її в єдиний запис.

Фактичним функціоналом даного сервісу є автоматизація пошуку всієї доступної інформації по CVE-ідентифікатору з додатковими функціями пошуку за вендорами, типами вразливостей, оцінкою критичності за метриками CVSS тощо. Також реалізовано збір та зберігання різноманітної статистики за вразливістю, наприклад, розподіл вразливостей за ступенем критичності (згідно з метрикою CVSS), розподіл вразливостей за вендорами ПЗ та ін. – зі зручним переходом до списку вразливостей, що задовольняють обраному критерію.

Таким чином, бази даних та реєстри вразливостей корисні широкому колу фахівців у галузі інформаційної безпеки. Мережеві адміністратори або співробітники, відповідальні за безпеку комп'ютерних систем організації, можуть своєчасно дізнатися з баз і реєстрів про появу нових загроз для систем, що захищаються, визначити пріоритетні заходи реагування на ці загрози.

При цьому для фахівців важливі оперативність оновлення баз даних вразливостей, зручність отримання цих оновлень і ступінь покриття обраним реєстром вразливостей як основних видів програмного забезпечення, що захищається, так і всієї безлічі вразливостей, виявлених для цього ПЗ. Також значущими характеристиками будуть наявність рекомендацій щодо усунення вразливостей і можливість визначення потенційних векторів атак на комп'ютерні системи, що захищаються.

Список використаних джерел:

1. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – 1999. – С. 5.

2. About CVE [Електронний ресурс] // The MITRE Corporation. – 2021. – Режим доступу до ресурсу: https://cve.mitre.org/about/index.html.

3. Vulnerability Notes Database [Електронний ресурс] // Carnegie Mellon University. – 2021. – Режим доступу до ресурсу: https://www.kb.cert.org/vuls/.

4. Exploit Database [Електронний ресурс] // OffSec Services Limited. – 2021. – Режим доступу до ресурсу: https://www.exploit-db.com/.

Ключові слова: вразливості, інформаційна безпека, бази даних, комп'ютерні системи.

Ключевые слова: уязвимости, информационная безопасность, базы данных, компьютерные системы.

Keywords: vulnerabilities, information security, databases, computer systems.

Плаксін Олександр Андрійович

Національний університет «Одеська юридична академія»,

студент 3-го курсу факультету кібербезпеки та інформаційних технологій

СУЧАСНІ КРИПТОГРАФІЧНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ

Криптографія – це наука про приховування інформації від несанкціонованих осіб.

Криптографія починає свою історію ще з далеких часів Римської імперії, коли був придуманий один із перших шифрів - Шифр Цезаря. З того часу криптографія просунулась далеко вперед і тепер використовується по всьому світу навіть у звичайнісіньких для нас речах: месенджерах, соціальних мережах, при перегляді ТБ, при серфінгу Інтернету тощо.

Зараз у світі існує безліч способів приховування інформації. Розберемо принцип їхньої дії, їх переваги та недоліки.