УДК 004.056.5

***Владислав БАГМЕТ[1], Віктор ДЗЯДИК[2]***

*[1]Західноукраїнський національний університет*
*[2]Галицький фаховий коледж ім. В'ячеслава Чорновола*

## GAME VULNERABILITIES ЯК ЗАГРОЗА КІБЕРБЕЗПЕКИ

**Вступ**. Баги та вразливості у комп'ютерних іграх є поширеним явищем, особливо в продуктах, що були випущені значний час тому. Така тенденція пояснюється тим, що розробники зосереджують основні ресурси на створенні нових проєктів, тоді як підтримка старих версій поступово скорочується. D наслідок цього популярні ігри з часом перетворюються на зручне середовище для дослідження та експлуатації вразливостей. До кола потенційних цілей кіберзловмисників належать як розробники, так і користувачі ігор, а в окремих випадках навіть організації, у межах яких ці користувачі працюють.

**Мета**: дослідити поширені вразливості у популярних продуктах гейміндустрії.

### 1. Загрози використання службових ПК з ігровим ПЗ

Комп'ютерна гра є програмним продуктом, тому може містити помилки в реалізації чи пропуски під час тестування. Наявність таких дефектів підтверджується публічними реєстрами (CVE), які фіксують відомі вразливості та їхню класифікацію за рівнем загрози. З метою дослідження цієї проблеми було проведено аналіз даних агрегатора вразливостей і перевірено інформацію щодо окремих проєктів на платформі Steam. Для прикладу було відібрано CVE, пов'язані з клієнтом гри Dota 2, середній рейтинг тяжкості яких за шкалою CVSS становив 7,8 із 10 [1].

Серед виявлених інцидентів, найсерйозніша була зафіксована у 2023 році внаслідок дослідження, проведеного фахівцями Avast: клієнт Dota 2 використовував застарілу версію рушія JavaScript (V8), яка містила вразливість, що дозволяла виконувати небажаний JavaScript-код на машині користувача. Наслідком дефектів може бути несанкціоноване виконання коду на комп'ютері жертви та повна компрометація її середовища.

Подібні ситуації відзначалися й у інших популярних проєктах. Так, для серії Counter-Strike виявлено кілька CVE із середнім значенням CVSS близько 7,76, а у грудні 2023 року було продемонстровано реалізацію XSS-вектору в контексті нової функції додавання зображень у чаті, що створювало можливості цілеспрямованих атак на користувачів. У випадку GTA Online дефект, позначений як CVE-2023-24059, було виявлено та виправлено на початку 2023 року. Цей збій дозволяв не лише отримати дані облікових записів, а й розміщувати шкідливе програмне забезпечення (ПЗ )на пристроях жертв.

Слід підкреслити, що запис у реєстрі CVE відображає лише вразливості, які вже стали загальновідомими і, як правило, були усунуті та опубліковані. Отже, загальна кількість дефектів у продуктах ігрової індустрії, ймовірно, значно перевищує кількість задокументованих CVE. Додатково практикою є те, що постачальники ПЗ іноді мають відомості про певні вразливості, але затримують їх

усунення через пріоритети розробки або інші операційні причини. Прикладом є ситуація з проєктом Call of Duty: Black Ops III (реліз 2015 року), де було задокументовано повідомлення про RCE-вразливості, які залишалися невиправленими тривалий час. В наслідок відсутності офіційних виправлень частина спільноти розробників-ентузіастів змушена була створювати власні модифікації та виправлення, доступні у відкритих репозиторіях.

Отже, із встановленим ігровим ПЗ з'являється низка ризиків: від локальних компрометацій окремих робочих станцій до потенційного розповсюдження загроз у внутрішній корпоративній мережі. Це обґрунтовує необхідність оцінки ризиків використання ігрового ПЗ на службі та запровадження політик контролю встановлення й оновлення програмного забезпечення, а також засобів виявлення й реагування на інциденти кібербезпеки.

## 2. Основні загрози ігровим акантам

Переважна більшість інцидентів із компрометацією облікових записів геймерів мають соціо-інженерний характер, причому найпоширенішим інструментом виступає фішинг. Атаки такого типу організовуються через чати, тематичні форуми та інші майданчики спільнот; їхня популярність пояснюється простотою реалізації та низькими витратами для зловмисника. Типовим прикладом є шахрайські схеми «я продав тобі, але ти не заплатив», які спрямовані на отримання облікових даних або доступу до платіжних інструментів жертви.

Технічно складніші вектори, що використовують програмні вразливості ігрових клієнтів або плагінів, зустрічаються рідше, оскільки вимагають відповідних навичок і часу на розробку експлойтів. Водночас такі атакувальні сценарії не є поодинокими і використання вразливостей може призводити до віддаленого виконання коду, підміни сесійних токенів або похищення облікових даних без прямого залучення користувача. Наслідком експлуатації вразливостей найчастіше стає крадіжка акаунтів, що, з огляду на розвиток внутрішньоігрових ринків, може мати значну матеріальну шкоду. Прикладом є інцидент 2022 року з відомим колекціонером предметів у грі серії Counter-Strike, в результаті якого було втрачене право розпоряджатися скінами загальною вартістю близько мільйонів доларів.

Значну загрозу також становить використання модифікованих або нелегально отриманих інсталяційних образів. Піратський софт, поширюваний через торренти й подібні ресурси, часто постачається разом із бекдорами та іншими типами шкідливого ПЗ, що робить його джерелом компрометації кінцевих пристроїв. У багатьох випадках саме завантаження та запуск модифікованих інсталяторів стають початковою точкою проникнення.

Окрему категорію ризиків формують користувацькі практики, які навмисно або мимоволі знижують рівень захисту кінцевої системи. Частина гравців вимикає антивірусні рішення або брандмауери, посилаючись на їх вплив на продуктивність або сумісність із грою. Інші користувачі взагалі відмовляються від активних засобів захисту. Ефективність таких налаштувань у сенсі підвищення продуктивності є предметом дискусій, натомість їхній внесок у підвищення вразливості системи виявлена й документована, зокрема зниження рівня захисту істотно збільшує ймовірність успішної компрометації облікових

записів і пристроїв.

Загрози ігровим акаунтам мають багатовимірний характер, від простих соціо-інженерних схем до технічно складних експлуатацій вразливостей і постачання шкідливого ПЗ разом із піратським контентом.Ускладнює ситуацію також поведінка користувачів, що іноді свідомо знижують заходи захисту. Це підкреслює необхідність комплексного підходу - поєднання технічних засобів, освітніх ініціатив для спільнот і проактивного моніторингу інцидентів.

### 3. Загрози додаткового ПЗ

Багато загроз також несуть у собі програми, які геймери активно використовують крім ігор. Вони теж можуть містити критичні дефекти безпеки, як це показано в таблиці 1.

Таблиця 1 – Вразливості ігрових майданчиків та спеціального ПЗ

| | |
|---|---|
| Steam та інші майданчики для розміщення ігор | Особливо небезпечна вразливість у Steam була виявлена у 2020 році. Використовуючи її, зловмисник міг захопити сотні тисяч комп'ютерів, не вимагаючи від геймерів натискати на шкідливий лист або посилання. На відміну від інших уразливостей, жертви несвідомо траплялися під вплив хакера. Для цього їм потрібно було просто увійти до гри. У 2023 році зловмисники зламали облікові записи сотні розробників на платформі Steam і додали до їхніх ігор шкідливе ПЗ. Але вендор швидко виявив проблему і повідомив про це користувачам. |
| Discord та інші утиліти для спілкування з командою | Повідомлень про проблеми у продукті чимало. Наприклад, минулого року розробник визнав витік даних 760 тис. користувачів, яка сталася з вини співробітника. |
| GeForce Experience, OBS Studio та інші програми для запису відео, оцінки FPS тощо. | У 2020 році розробник GeForce Experience залатав відразу дві серйозні дірки. Одна з уразливостей (CVE-2020-5977) отримала CVSS 8,2 і могла призвести до безлічі шкідливих атак на порушені системи, включаючи виконання коду, відмову в обслуговуванні, підвищення привілеїв та розкриття інформації. |
| AutoHotKey та аналоги для налаштування кнопок клавіатури та миші | З його допомогою злочинці поширювали трояни для віддаленого доступу до пристроїв жертв, у тому числі Revenge RAT, LimeRAT, AsyncRAT, Houdini та Vjw0rm. |
| Spotify та інші сервіси для прослуховування музики під час гри | У 2020 році через виток даних Spotify скинув 350 тис. паролів користувачів. Хоча в офіційній заяві власник продукту повідомив, що проблема торкнулася лише невеликої частини акаунтів. |

CVE-2020-5977 - уразливість типу «небезпечний/неконтрольований пошук шляху завантаження модулів» (untrusted search path) в компоненті, що

використовує середовище виконання Node.js. Через цю слабину процес, який завантажує модулі Node.js (через require() / import), може підхопити шкідливий модуль із непередбачуваного або керованого зловмисником каталогу. Унаслідок цього можливе виконання довільного коду в контексті вразливого процесу, що може призвести до локальної компрометації системи.

Схема вразливості CVE-2020-5977 приведена на рисунку 1.

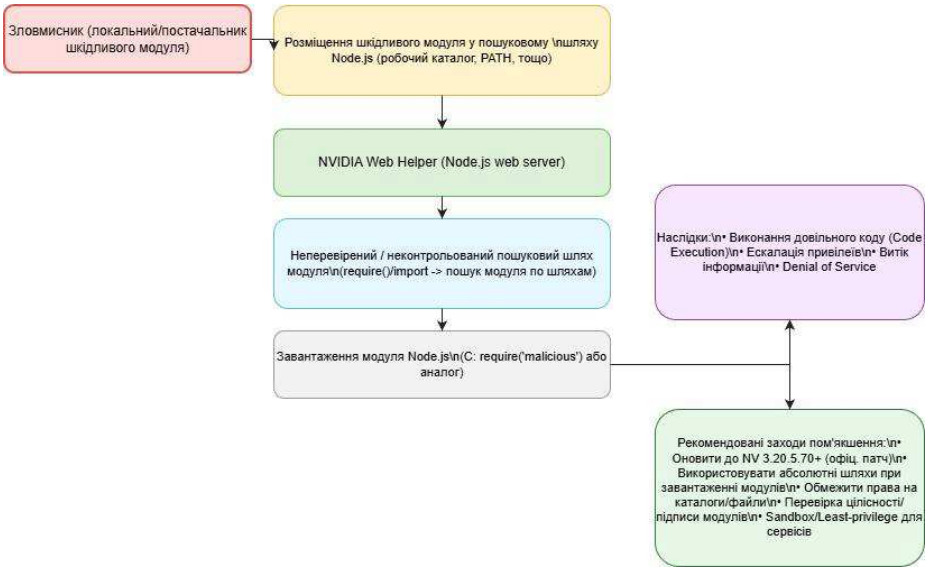


Рисунок 1 - Схема вразливості CVE-2020-5977

CVE-2020-5977 належить до класу вразливостей, які використовують недоліки в управлінні шляхами завантаження модулів у середовищах виконання, таких як Node.js. Механізм експлуатації є концептуально простим, проте практичні наслідки можуть бути критичними. Найефективнішими заходами захисту є своєчасне оновлення ПЗ, управління правами доступу, використання перевірок цілісності модулів та впровадження контролю завантажених компонентів у рантаймі.

**Висновок.** Безпека відеоігор є багатовимірною проблемою, що поєднує технічні вразливості програмного коду, ризики соціальної інженерії та операційні загрози, пов'язані з практиками розповсюдження та використання ПЗ. Наслідки експлуатації вразливостей охоплюють як індивідуальні втрати користувачів, так і бізнес-ризики для розробників та їхньої інфраструктури. Ефективна протидія потребує комбінованого підходу, що включає безпечну розробку, регулярне патчування, контроль цілісності файлів і жорстке управління правами доступу. Додатково необхідні механізми та інструменти моніторингу (EDR, HIDS, SIEM), а також просвітницькі заходи для користувацької спільноти щодо фішингу та безпечних практик. Лише системне поєднання технічних, організаційних і правових заходів здатне істотно знизити експлуатаційний ризик і підтримати довгострокову стійкість ігрової екосистеми.

**Перелік використаних джерел.**

1. CVE-2015-7985. [Електронний ресурс]. - Режим доступу: https://nvd.nist.gov/vuln/detail/CVE-2015-7985.

2. CVE-2020-5977. [Електронний ресурс]. - Режим доступу: https://nvd.nist.gov/vuln/detail/CVE-2020-5977.