

# КЛАСИФІКАЦІЯ ВРАЗЛИВОСТЕЙ БІНАРНИХ ФАЙЛІВ

І. О. Трайдакало<sup>1, а</sup>

<sup>1</sup>Національний технічний університет України «Київський політехнічний інститут»

## Анотація

В роботі проаналізовано підходи до виявлення вразливостей програмного забезпечення та причини їх виникнення та запропоновано власну класифікацію вразливостей.

**Ключові слова:** бінарні вразливості, класифікація бінарних вразливостей, захист програмного забезпечення, інформаційна безпека

## Вступ

Проблема захисту програмного забезпечення (ПЗ) – одна з найактуальніших проблем захисту інформації (ЗІ). Визначальним фактором, що істотно впливає на рівень успішності її вирішення, є детальне вивчення та аналіз вразливостей ПЗ. Підсумкові результати цього аналізу часто подаються у формі класифікації вразливостей. Це пояснюється тим, що вдала класифікація вразливостей, як правило, є ключовою умовою успішної розробки механізмів захисту ПЗ.

Зазвичай така класифікація базується на тих чи інших принципах, введених відповідно до інтуїції дослідника, певних традиційних схем та підходів. Часто подібні класифікації поєднують різнотипні вразливості, наприклад, вразливості у Web-застосуваннях розглядаються сумісно із вразливостями в бінарних файлах.

## 1. Методика досліджень

**Вразливості ПЗ** – критичні помилки, не виявлені в ході тестування і не декларовані специфікацією розробника або закладені навмисно, що надають зловмисникам виняткові можливості по розголошенню інформації, її модифікації, блокування використання та безостаточно знищенню без можливості відновлення.

Для виявлення вразливостей ПЗ існує багато підходів: системи статичного аналізу вихідного коду, системи динамічного аналізу вихідного коду, перевірка коректності анотацій користувача, автоматизація експертного аудиту та верифікація обмеженого вихідного коду. Опираючись на підходи виявлення різних вразливостей в ході виконання роботи було проаналізовано та досліджено причини виникнення відомих вразливостей та помилок ПЗ.

## 2. Результати досліджень

В результаті досліджень було запропоновано власний варіант класифікацій вразливостей у бінарних файлах:

- 1) *Вразливості disasm* – це вразливості на рівні асемблерівського коду.
- 2) *Pointer vuln* – це вразливості пов'язані з суттю покажчика і роботою Memory Manager.
- 3) *Control Flow Graph (CFG)* – вразливості які виникають при побудові CFG.
- 4) *Errate* – вразливості в архітектурі процесора.
- 5) *Format String Vuln (FSV)*.
- 6) *Logic* – логічні Вразливості у рівні архітектури ПЗ.

## Висновки

В даній роботі представлено нову класифікацію вразливостей ПЗ. Для більшості з вразливостей проведений детальний аналіз особливостей їх структур, умов виникнення та використання. Наведений матеріал може бути корисним при створенні та дослідженні математичних моделей для різних типів вразливостей.

## Перелік використаних джерел

1. Peter Mell, Karen Scarfone. A Complete Guide to the Common Vulnerability Scoring System Version 2.0 [Електронний ресурс] // first.org. – 2007. <http://www.first.org/cvss/cvss-guide.html>
2. Format String Vulnerability [Електронний ресурс] // tech-faq.com. – 2010. <http://www.tech-faq.com/format-string-vulnerability.html>
3. Джек Козіол, Девід Лічфілд, Дейв Ейтел. Ми-стецтво злому та захисту систем. – Пітер, 2006. – 276 с.

<sup>а</sup>igor\_traydakalo@gmail.com