УДК 004.056(75)

Нікіта Прокопчук
Галина Крайнічук (Шелепало)

АНАЛІЗ ТИПОВИХ ВРАЗЛИВОСТЕЙ КОНФІГУРАЦІЙ СЕРВІСІВ IAM, S3 ТА EC2 У СЕРЕДОВИЩІ AWS

Вінницький національний технічний університет

Анотація. *У роботі систематизовано типові вразливості конфігурацій хмарних сервісів Amazon Web Services: управління ідентифікацією та доступом (IAM), об'єктного сховища (S3) та обчислювальних ресурсів (EC2). Для кожної категорії описано сценарії експлуатації, реальні інциденти та кількісні оцінки критичності за шкалою CVSS v3.1. Сформовано ієрархічну класифікацію загроз та обґрунтовано пріоритетність заходів із мінімізації ризиків у контексті моделі спільної відповідальності AWS.*

Ключові слова: AWS, IAM, S3, EC2, некоректна конфігурація, вразливість, CVSS, хмарна безпека, аналіз ризиків.

Abstract. *The paper systematises typical configuration vulnerabilities of Amazon Web Services cloud services: Identity and Access Management (IAM), Simple Storage Service (S3), and Elastic Compute Cloud (EC2). For each category, exploitation scenarios, real-world incidents, and quantitative criticality scores according to the CVSS v3.1 scale are described. A hierarchical threat classification is proposed and the priority of risk mitigation measures is justified within the AWS Shared Responsibility Model.*

Keywords: AWS, IAM, S3, EC2, misconfiguration, vulnerability, CVSS, cloud security, risk analysis.

Вступ

Модель спільної відповідальності AWS (Shared Responsibility Model) покладає на користувача повний контроль над безпекою конфігурацій хмарних сервісів [1]. Попри широку доступність офіційних рекомендацій, 68 % усіх хмарних інцидентів у 2024 році спричинені саме помилками налаштувань, а не вразливостями самої платформи [2]. Ключовими об'єктами компрометації залишаються три сервіси: Identity and Access Management (IAM) як точка входу для більшості атак на облікові дані, Simple Storage Service (S3) як джерело масштабних витоків даних та Elastic Compute Cloud (EC2) як обчислювальний ресурс, що піддається мережевим атакам. Систематизація типових вразливостей цих сервісів із кількісною оцінкою критичності дозволяє сформувати обґрунтовану пріоритетність заходів захисту [3].

Вразливості сервісу IAM

Сервіс IAM є глобальним механізмом авторизації, тому його компрометація відкриває доступ до всієї інфраструктури акаунта. Найкритичнішою вразливістю є відсутність багатофакторної автентифікації (MFA) у поєднанні з довготривалими ключами доступу (Access Keys). Якщо статичний ключ потрапляє до публічного репозиторію GitHub або викрадається через фішинг, зловмисник отримує повну карту інфраструктури через команди aws ec2 describe-instances, aws s3 ls, aws iam list-users без жодних додаткових бар'єрів. За даними Palo Alto Networks Unit 42, у 58 % досліджених AWS-акаунтів виявлено принаймні одного користувача з привілеями, що суттєво перевищують службову необхідність [2]. Окремий вектор становлять надлишкові політики з конструкцією «Action»: «*» на «Resource»: «*», які нерідко мігрують із тестових конфігурацій у продуктивне середовище. За шкалою CVSS v3.1 відсутність MFA оцінюється у 8.8 балів (High), а надлишкові ключі доступу старші 90 днів – у 4.5 (Medium) [4].

Вразливості сервісу S3

Головним вектором атак на S3 є ненавмисне надання публічного доступу до бакетів із конфіденційними даними. Зловмисники застосовують методи перебору типових імен (company-backup, static-assets, logs) та аналіз SSL-сертифікатів через сервіс crt.sh для виявлення асоційованих субдоменів. Інструменти на кшталт S3Scanner перевіряють сотні імен бакетів за секунду, після чого звичайний HTTP GET-запит до відкритого ресурсу повертає повний список об'єктів без автентифікації. Показовим є витік даних Capital One у 2019 році: через SSRF-вразливість веб-застосунку зловмисник отримав доступ до сервісу метаданих EC2, викрав ключі IAM-ролі та скомпрометував понад 100 мільйонів

записів клієнтів [5]. Додатковим фактором ризику є відсутність шифрування даних у стані спокою: навіть увімкнена опція «Block Public Access» не захищає від витоку, якщо Bucket Policy явно надає доступ стороннім принципалам. CVSS-бал публічного доступу до S3 становить 9.8 (Critical), відсутності шифрування – 5.3 (Medium) [4].

Вразливості сервісу EC2

Для EC2 основним вектором є некоректне налаштування груп безпеки (Security Groups): відкриття портів SSH (22) або RDP (3389) для діапазону 0.0.0.0/0 дозволяє будь-якому користувачу інтернету ініціювати з'єднання з інстансом. Пошукові системи Shodan та Censys індексують такі інстанси автоматично, після чого застосовуються інструменти брутфорсу або модулі Metasploit для експлуатації вразливостей конкретних версій сервісів. Окрему загрозу становить відсутність прив'язаних IAM-ролей до EC2-інстансів: якщо розробники зберігають статичні ключі в змінних середовища, зловмисник після отримання доступу до інстансу витягує їх через звернення до сервісу метаданих за адресою 169.254.169.254. У 2023–2024 рр. набув поширення сценарій прихованого криптомайнінгу: після компрометації запускаються процеси XMRig із навантаженням CPU до 100 % та аномальним вихідним трафіком на майнінг-пули, що без автоматизованого моніторингу може залишатися непоміченим тижнями [3]. CVSS-бал відкритого порту управління становить 8.6 (High), відсутності IAM-ролі – 3.9 (Low) [4].

Висновки

Проведений аналіз демонструє, що вразливості конфігурацій IAM, S3 та EC2 мають чітку ієрархію критичності: найвищий пріоритет усунення отримують публічний доступ до S3-бакетів (CVSS 9.8) та відсутність MFA в IAM (CVSS 8.8), далі – відкриті порти управління EC2 (CVSS 8.6). Спільною рисою всіх категорій є кумулятивний ефект: поєднання двох і більше некритичних налаштувань (відсутність MFA + надлишкові права + незашифрований S3) створює ланцюгову вразливість із катастрофічними наслідками, що підтверджується реальними інцидентами [5]. Отримана класифікація слугує основою для формування бази правил автоматизованих засобів аудиту класу CSPM та визначення пріоритетів у процесах безперервного моніторингу хмарної інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. AWS Shared Responsibility Model / Amazon Web Services, Inc. URL: https://aws.amazon.com/compliance/shared-responsibility-model/ (дата звернення: 24.03.2026).
2. Palo Alto Networks Unit 42. Cloud Threat Report 2024. URL: https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research (дата звернення: 02.03.2026).
3. Скоринович Б. В., Лах Ю. В. Аналіз методів моніторингу стану безпеки в хмарному середовищі. Сучасний захист інформації. 2025. № 1(61). С. 298–310. DOI: 10.31673/2409-7292.2025.012256.
4. NVD – CVSS v3 Calculator / National Institute of Standards and Technology. URL: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (дата звернення: 27.05.2026).
5. Top Threats to Cloud Computing: Egregious Eleven / Cloud Security Alliance. 2022. URL: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/ (дата звернення: 24.03.2026).

Прокопчук Нікіта Павлович – студент групи БКС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця. E-mail: nikusha1305@gmail.com.

Шелепало (Крайнічук) Галина Василівна – к.фіз-мат.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця. E-mail: hv.shelepalo@vntu.edu.ua

Prokopchuk Nikita Pavlovich – student of the group BKS-22b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia. E-mail: nikusha1305@gmail.com.

Shelepalo (Krainichuk) Halyna Vasylivna – Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Information Security, Vinnytsia National Technical University, Vinnytsia. E-mail: hv.shelepalo@vntu.edu.ua