Engineer

CVE

публічний перелік, що дає кожній відомій вразливості номер

Що це таке

CVE, що розшифровується як Common Vulnerabilities and Exposures, — це публічний каталог оприлюднених вразливостей кібербезпеки, де кожна має свій запис CVE (CVE Record). Програма CVE описує свою місію як виявлення, визначення та каталогізацію таких вразливостей, щоб двоє людей або два інструменти могли послатися на ваду й бути певними, що мають на увазі ту саму. Цим словом називають і програму, і перелік, а побіжно й окремий запис, як у фразі «у цій бібліотеці дві відкриті CVE».

Кожен запис має ідентифікатор CVE (CVE ID). Його формат — префікс `CVE`, рік із чотирьох цифр і порядковий номер із чотирьох або більше цифр, тож `CVE-1999-0067`, `CVE-2019-12345` і `CVE-2021-7654321` однаково коректні; верхньої межі довжини порядкового номера програма не встановлює. Рік — це рік, коли ідентифікатор зарезервували, або рік, коли вразливість оприлюднили. Програма окремо наголошує, що рік не вказує, коли вразливість виявили.

Ідентифікатори не видає одне центральне бюро. Органи нумерації CVE (CVE Numbering Authorities, CNA) — це постачальники, дослідники, проєкти з відкритим кодом, команди реагування на комп'ютерні надзвичайні ситуації, оператори онлайн-сервісів, організатори програм винагород за знайдені вразливості та консорціуми, яким програма дозволила призначати ідентифікатори й публікувати записи, кожному в межах власної сфери. Кожен запис CVE до переліку додає один із CNA; щоб стати таким органом, не треба ні платити внесок, ні підписувати договір, а з 2016 року програма активно залучає нових.

Запис проходить три стани. Спершу він Reserved: CNA взяв ідентифікатор, і причетні сторони використовують його, щоб координувати ранню роботу над вразливістю до її оприлюднення. Станом Published запис стає, коли CNA

заповнив щонайменше ідентифікатор, короткий опис, уражені продукти й версії та публічне посилання. Якщо ідентифікатор більше не слід використовувати, запис переходить у стан Rejected і лишається в переліку, щоб кожен, хто має цей ідентифікатор, бачив, що той недійсний.

Ідея з’явилася 1999 року. Двоє інженерів MITRE, Девід Е. Манн і Стівен М. Крісті, представили концепцію в доповіді на семінарі в Університеті Пердью в січні 1999 року, а у вересні того ж року перелік став публічним і містив 321 запис.

Застосуйте поняття до рішення

Застосуйте «Що таке CVE?» до конкретного рішення. Ми можемо пов'язати поняття із системою, яку ви створюєте або купуєте. Облікові записи, паролі й права налаштовані так, щоб доступ відповідав роботі, а звільнені втрачали його того ж дня.

Переглянути наші послуги Зв'язатися з нами →

Перевірте припущення за терміном

Використайте пояснення та пов'язані роботи, щоб сформулювати запитання для проєкту. Ми можемо перевірити припущення разом до вибору інструмента. Написала 1 000 правил RBAC для Linux-серверів — 1,000 правил доступу написано, щоб усунути вразливість

Написала 1 000 правил RBAC для Linux-серверів Зв'язатися з нами →

Чому це важливо

Звіт про вразливість корисний лише тоді, коли читач може визначити, чи йдеться в ньому про ту саму проблему, що й в іншому звіті. Ідентифікатор CVE це питання знімає: два бюлетені безпеки, знахідка сканера й задача в трекері з однаковим ідентифікатором стосуються однієї вади. Чимало великих постачальників операційних систем вказують ідентифікатори CVE у своїх бюлетенях безпеки, тож ідентифікатор є в усіх від моменту, коли про проблему оголошено, а продукти й сервіси безпеки по всьому світу вбудовують записи CVE у свої звіти.

Інші сервіси побудовано на основі переліку, а не поряд із ним. Американська National Vulnerability Database (NVD), яку NIST запустив 2005 року, — окрема програма, що спирається на записи CVE й додає до кожного власний аналіз. Каталог Known Exploited Vulnerabilities (KEV) агентства CISA збирає вади, які, як помічено, зловмисники вже використовують, і кожен запис у ньому ідентифіковано записом CVE та має посилання на нього.

Найкорисніше знати про CVE те, чим CVE не є. Це не оцінка критичності: нею займається Common Vulnerability Scoring System, CVSS, окремий стандарт, який веде FIRST — американська неприбуткова організація, що має на меті

допомагати командам реагування в галузі комп’ютерної безпеки в усьому світі. CVSS версії 4.0 оцінює вразливість від 0 до 10 за чотирма групами показників — Base, Threat, Environmental і Supplemental — і переводить число в шкалу None, Low, Medium, High і Critical, де Critical охоплює діапазон від 9,0 до 10,0. Формат запису CVE (CVE Record Format) дозволяє CNA додати оцінку CVSS до свого запису, але оцінка належить CVSS, а не ідентифікатору: одна вада може мати різні оцінки від різних видавців або не мати жодної.

Це також не клас слабкостей. Common Weakness Enumeration, CWE, — це перелік слабкостей, який розробляє спільнота: умови в програмному забезпеченні, мікропрограмах, апаратному забезпеченні чи сервісі, які за певних обставин можуть відкрити шлях до вразливості. Програма CVE описує CWE як першопричини записів CVE. CVE називає одну ваду в одному продукті; CWE називає тип помилки, що за нею стоїть. SQL-ін’єкція, наприклад, — це слабкість CWE-89, і кожен продукт, у якому знайшли саме цю помилку, отримує власний ідентифікатор CVE.

Як це виглядає на практиці

Shellshock, вада в Bash 2014 року, показує всі три системи поруч. cve.org показує свої записи у форматі CVE Record Format, побудованому на JSON, і початок цього запису виглядає так (частину полів прибрано, порядок змінено):

```
{
  "dataType": "CVE_RECORD",
  "dataVersion": "5.1",
  "cveMetadata": {
    "cveId": "CVE-2014-6271",
    "assignerShortName": "debian",
    "state": "PUBLISHED",
    "dateReserved": "2014-09-09T00:00:00.000Z",
    "datePublished": "2014-09-24T18:00:00.000Z",
    "dateUpdated": "2025-10-22T00:05:36.342Z"
  }
}
```

Debian як CNA зарезервував ідентифікатор 9 вересня 2014 року й опублікував запис через п’ятнадцять днів. В описі сказано, що Bash до версії 4.3 включно обробляє текст, який іде після визначення функції у значенні змінної середовища, тож віддалений зловмисник може виконати довільний код через спеціально підготовлене середовище. У записі також зазначено,

що перше виправлення було хибним, а частина, яка лишилася відкритою після нього, отримала власний ідентифікатор, CVE-2014-7169. Команди, що оновилися один раз і на цьому зупинилися, лишалися вразливими.

Далі запис містить контейнери з трьох різних джерел. Контейнер CNA містить опис і посилання від Debian. CVE Program Container додає власні посилання. Третій, від Authorized Data Publisher під назвою CISA ADP Vulnrichment, додає те, чого сам ідентифікатор CVE не повідомляє:

```
{
  "cvssV3_1": {
    "version": "3.1",
    "vectorString": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H",
    "baseScore": 9.8,
    "baseSeverity": "CRITICAL"
  }
}
```

Рядок вектора розкриває логіку оцінки 9,8: атака через мережу, низька складність, жодних привілеїв і жодної дії користувача, високий вплив на конфіденційність, цілісність і доступність. Той самий контейнер зіставляє ваду з CWE-78, класом слабкостей для впровадження команд операційної системи, і фіксує, що 28 січня 2022 року CISA додало її до каталогу KEV. Отже, один запис містить ідентифікатор від програми CVE, оцінку за версією CVSS, яку публікує FIRST, і клас слабкості з CWE — кожне з окремого джерела, і кожне відповідає на своє питання.

У щоденній роботі ідентифікатори CVE важать не як текст для читання, а як ключі. Наша сторінка про безпеку описує цей порядок: з чого складається кожна система, записують, і цей список перевіряють за опублікованими бюлетенями безпеки, а не покладаються на нього через те, що він працював раніше. Саме ідентифікатор CVE дає змогу простежити знахідку такої перевірки назад до бюлетеня і вперед до оновлення, яке її закриває.

Де виникають проблеми

Оцінку сприймають як ризик. Коли ніхто не задає значень Threat і Environmental, специфікація CVSS 4.0 підставляє стандартні значення, що припускають найгірше, і зазначає, що NVD та супровідники продуктів зазвичай публікують лише оцінку Base. Оцінка 9,8 для компонента, до якого

не дістатися ззовні, для вас не є 9,8. Позначайте оцінки так, як просить специфікація: CVSS-B лише для Base і CVSS-BTE, коли застосовано значення Threat і Environmental, — і додавайте значення Environmental для власних систем, перш ніж розставляти пріоритети.

CVE, CVSS і CWE плутають між собою. «CVE на 9,8» змішує ідентифікатор з оцінкою, а «та CVE про SQL-ін'єкцію» змішує ваду з класом вад. Тримайте ці три речі окремо в задачах і звітах: ідентифікатор — з CVE, оцінку разом з її версією — з CVSS, першопричину — з CWE.

Число наводять без вектора. FIRST вимагає від кожного, хто публікує дані CVSS, наводити і оцінку, і рядок вектора, щоб інші бачили, як оцінку отримано. Голе число неможливо перевірити, порівняти між версіями CVSS чи пристосувати до ваших умов. Фіксуйте повний вектор разом із префіксом `CVSS:3.1/` або `CVSS:4.0/`, який називає версію.

Рік читають як дату виявлення. Рік в ідентифікаторі показує, коли ідентифікатор зарезервували або коли ваду оприлюднили. Ідентифікатор 2014 року може описувати код, випущений у 1990-х, а вада, знайдена в грудні, може отримати номер наступного року. Для дат використовуйте поля запису `dateReserved` і `datePublished`, а не ідентифікатор.

Розраховують на чотири цифри. Порядковий номер має чотири або більше цифр без верхньої межі, тож шаблон на кшталт `CVE-\d{4}-\d{4}` мовчки обрізає довші ідентифікатори. Натомість перевіряйте відповідність `^CVE-[0-9]{4}-[0-9]{4,}$` і обробляйте ідентифікатор як рядок, а не число, щоб початкові нулі не губилися.

Запис Rejected вважають зниклим. Відхилений ідентифікатор навмисно лишається в переліку, щоб повідомити користувачам, що він недійсний. Інструменти, які його ігнорують або рахують відкритою знахідкою, вводять в оману, кожен у свій бік. Читайте поле `state` і обробляйте `REJECTED` явно.

Запис вважають завершеним. Запис Shellshock востаннє змінювали в жовтні 2025 року, через одинадцять років після публікації, а до каталогу KEV його додали в січні 2022 року. Специфікація CVSS описує свою групу Threat як характеристики вразливості, що змінюються з часом. Регулярно перечитуйте записи, що стоять за знахідками, які ви прийняли, а не виправили.

Зупиняються на першому виправленні. Для Shellshock знадобився другий ідентифікатор, бо перше виправлення залишило частину вади відкритою. Шукайте в описі й посиланнях кожного запису подальші ідентифікатори і закривайте знахідку лише тоді, коли вирішено всі ідентифікатори, що згадують компонент.

Відсутність CVE сприймають як відсутність вразливості. CVE охоплює вразливості, які оприлюднено і яким CNA у межах своєї сфери призначив ідентифікатор. Вада у вашому власному коді не має CVE, доки хтось про неї не повідомить і не оприлюднить її. Сканування залежностей за переліком покриває те, що знайшли інші; власний код потребує власного статичного аналізу, рецензування й тестування.

Що почитати далі

- CVE Program: Overview — місія програми, запис CVE і партнери, які призначають ідентифікатори та публікують записи.
- CVE Program: Process — формат ідентифікатора, мінімальний вміст запису та три його стани.
- CVE Program: Related Efforts — як NVD, CVSS, каталог KEV і CWE пов’язані з CVE і чим від нього відрізняються.
- Common Vulnerability Scoring System v4.0: Specification Document — групи показників FIRST, позначення оцінок і якісна шкала критичності.
- CVE Record Format — JSON-визначення того, як побудовано запис, у версії, яку використовує CVE Services.
- CVE Program: FAQs (archive)

Словник

Обирайте за фактичними умовами

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Зробіть термінологію практичною

Запитайте, як «Що таке CVE?» стосується вашої організації. Конкретного прикладу з поточної системи достатньо для початку розмови.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/glossary/cve/