CVE(Common Vulnerabilities and Exposures**)**

It is a publicly available list of known cybersecurity vulnerabilities and exposures that provides a unique identifier for each issue.

Goal : is to standardize the naming and tracking of vulnerabilities to facilitate easier information sharing and collaboration among cybersecurity professionals and organizations.

Eg. CVE entry looks like this:
CVE-YYYY-NNNNN

CVE: Common Vulnerabilities and Exposures
YYYY: The year the CVE was assigned
NNNNN: A unique identifier for the vulnerability

DevSecOps organization & projects

CVE(Common Vulnerabilities and Exposures**)**

For the latest CVEs, you can visit the NVD website https://nvd.nist.gov/
Some well known CVE for eg.

1) **CVE-2021-34527 (PrintNightmare):**

Description: A critical vulnerability in the Windows Print Spooler service that allowed remote code execution.
Impact: The vulnerability was actively exploited before a complete fix was available.
Year: 2021

2) **CVE-2021-44228 (Log4Shell / Log4j vulnerability):**

Description: A critical remote code execution vulnerability in Apache Log4j 2.x, which allowed attackers to execute arbitrary code on affected systems by sending a specially crafted request to the application's log4j socket server.
Impact: The vulnerability had a wide-ranging impact due to the popularity of Log4j in various Java applications and web servers. It was actively exploited by threat actors to gain unauthorized access to systems and launch further attacks.
Year: 2021

DevSecOps organization & projects