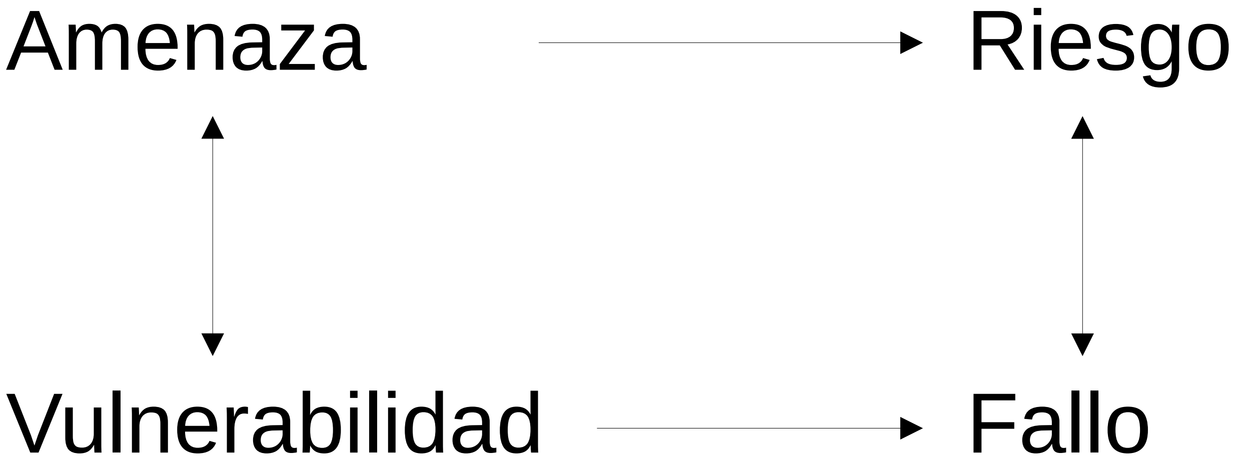
Criptografía
y
Seguridad

Vulnerabilidades

¿Que es una vulnerabilidad?



Amenaza

Riesgo

Vulnerabilidad

Fallo

Una vulnerabilidad informática es **cualquier fallo o error** en un sistema que puede ser aprovechado para comprometer su politica de seguridad.

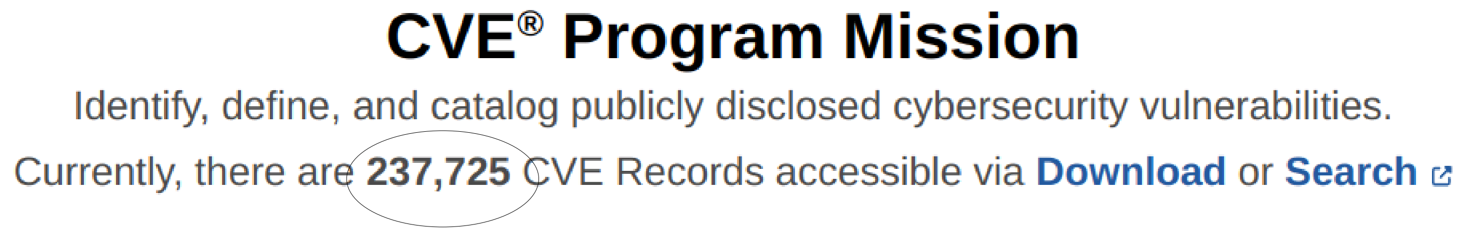
Dimensiones de vulnerabilidades

Taxonomia Seven Kingdoms (Tsipenyk)

- Input Validation and Representation
- API Abuse
- Security Features
- Time and State
- Error Handling
- Code Quality
- Encapsulation

Common Vuln and Exposures (CVE)

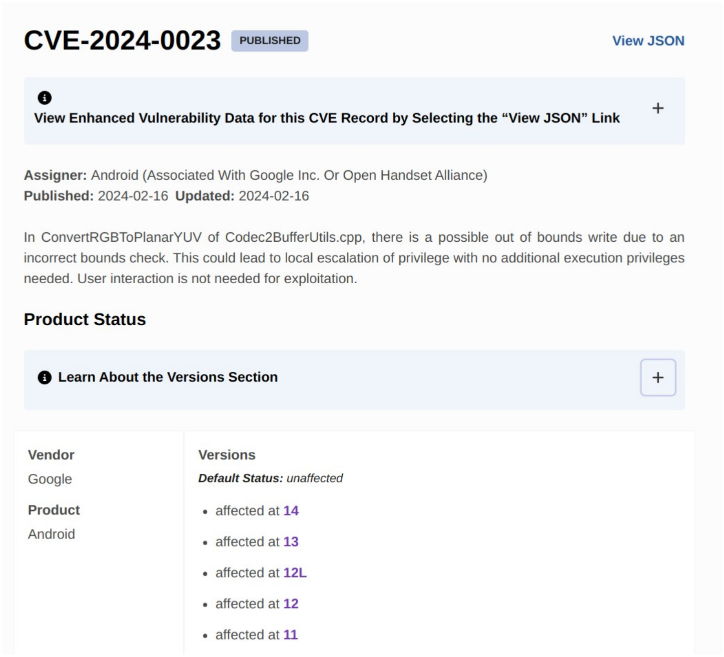
- Base de datos publica de vulnerabilidades concretas: https://www.cve.org/



CVE® Program Mission

Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

Currently, there are **237,725** CVE Records accessible via **Download** or **Search**



CVE-2024-0023 PUBLISHED

View JSON

View Enhanced Vulnerability Data for this CVE Record by Selecting the “View JSON” Link +

Assigner: Android (Associated With Google Inc. Or Open Handset Alliance)
Published: 2024-02-16 **Updated:** 2024-02-16

In ConvertRGBToPlanarYUV of Codec2BufferUtils.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

Product Status

Learn About the Versions Section +

Vendor	Versions
Google	***Default Status:*** *unaffected*
Product	- affected at 14 - affected at 13 - affected at 12L - affected at 12 - affected at 11
Android	

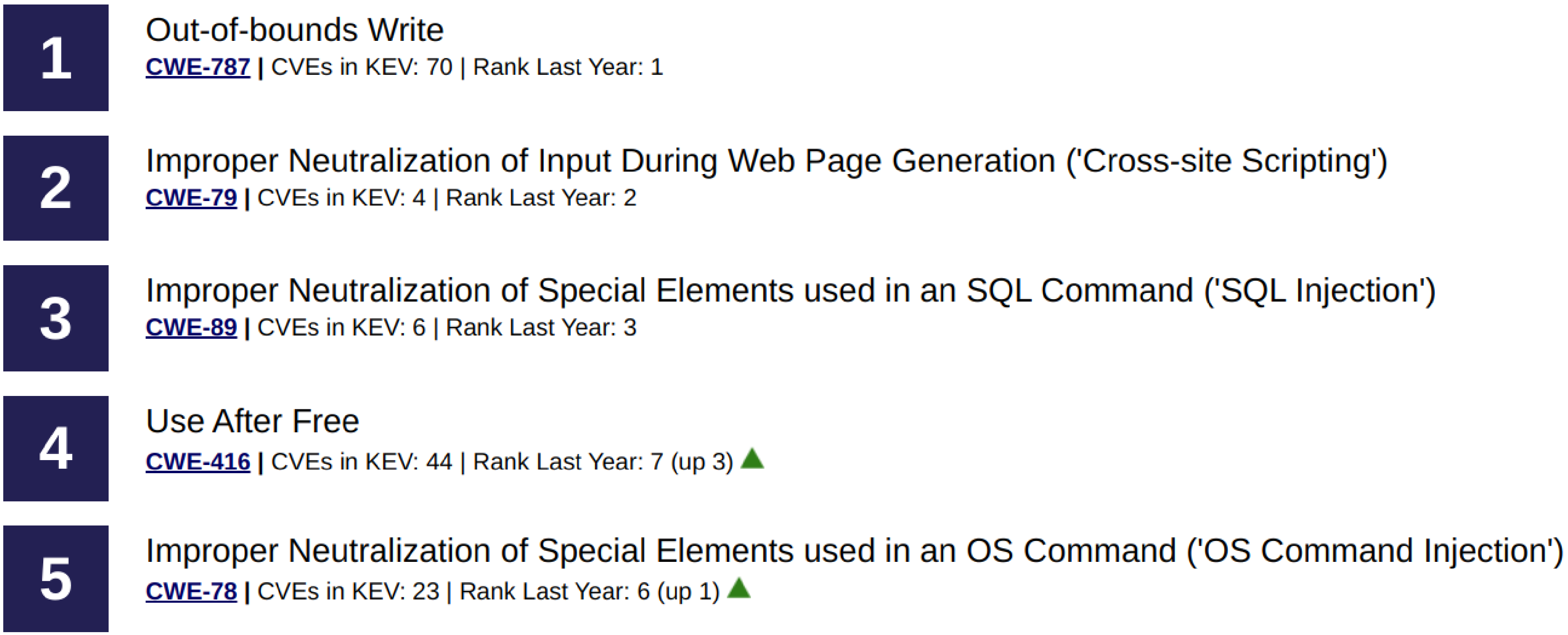
Causas raiz: CWE

(Common Weakness Enumeration)
https://cwe.mitre.org/index.html

- Taxonomia de amenazas que pueden convertirse en vulnerabilidades
- Es jerarquica, parte de categorias y llega a casos propios de por ejemplo un lenguaje de programacion en particular
- Mas de 1000 CWEs

- Una vulnerabilidad se correlaciona con una o mas CWEs

CWE – Top 25 (2023)



1

Out-of-bounds Write
CWE-787 | CVEs in KEV: 70 | Rank Last Year: 1

2

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-79 | CVEs in KEV: 4 | Rank Last Year: 2

3

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-89 | CVEs in KEV: 6 | Rank Last Year: 3

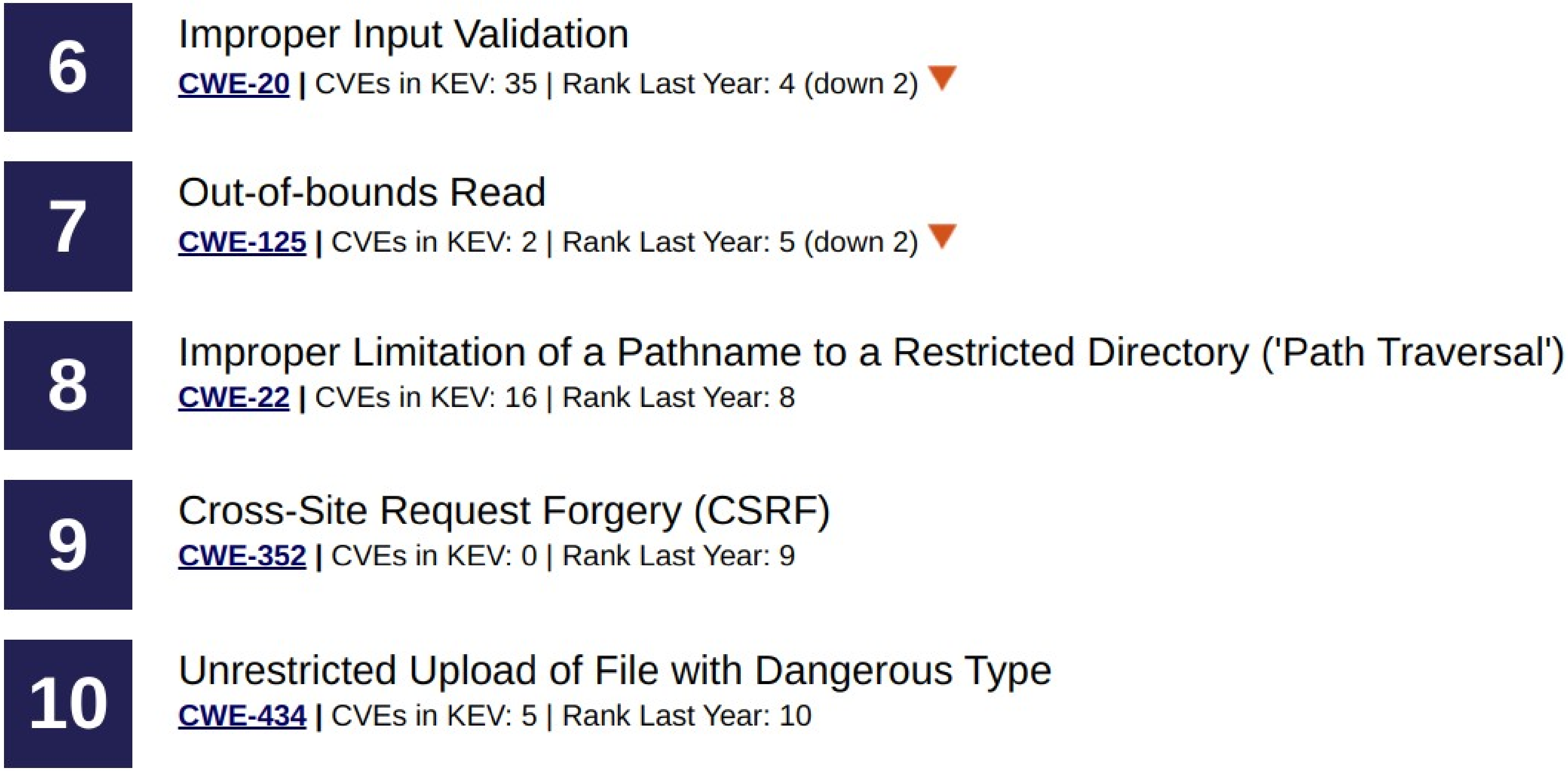
4

Use After Free
CWE-416 | CVEs in KEV: 44 | Rank Last Year: 7 (up 3) ▲

5

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-78 | CVEs in KEV: 23 | Rank Last Year: 6 (up 1) ▲

CWE – Top 25 (2023)



6 Improper Input Validation
CWE-20 | CVEs in KEV: 35 | Rank Last Year: 4 (down 2) ▼

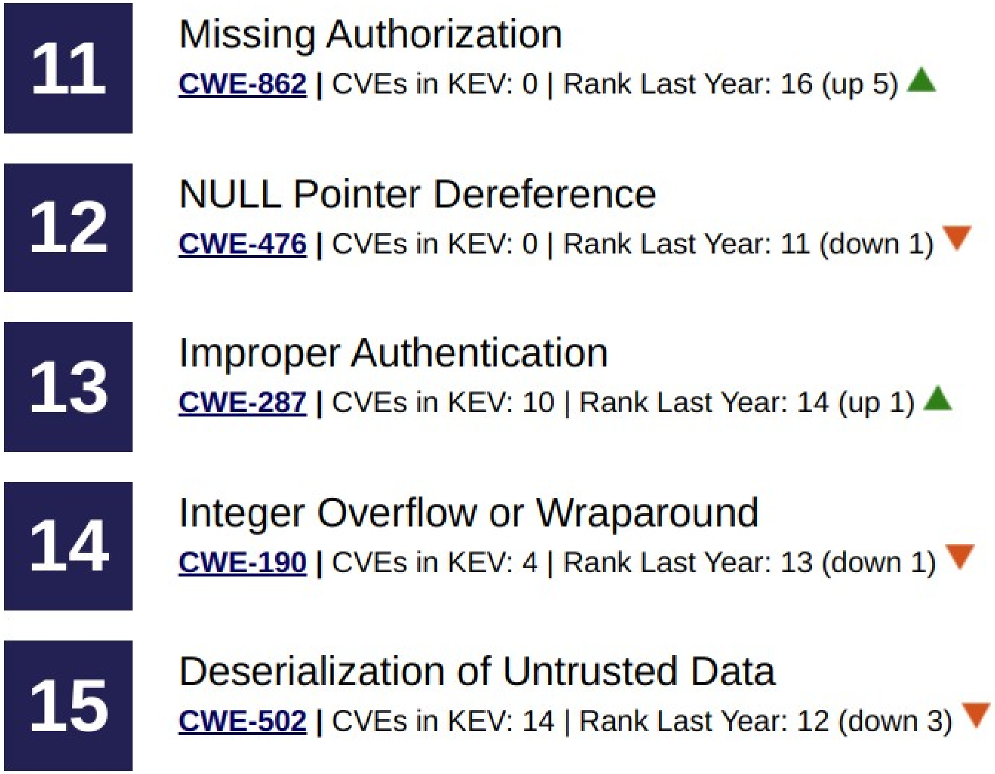
7 Out-of-bounds Read
CWE-125 | CVEs in KEV: 2 | Rank Last Year: 5 (down 2) ▼

8 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-22 | CVEs in KEV: 16 | Rank Last Year: 8

9 Cross-Site Request Forgery (CSRF)
CWE-352 | CVEs in KEV: 0 | Rank Last Year: 9

10 Unrestricted Upload of File with Dangerous Type
CWE-434 | CVEs in KEV: 5 | Rank Last Year: 10

CWE – Top 25 (2023)



11 Missing Authorization
CWE-862 | CVEs in KEV: 0 | Rank Last Year: 16 (up 5) ▲

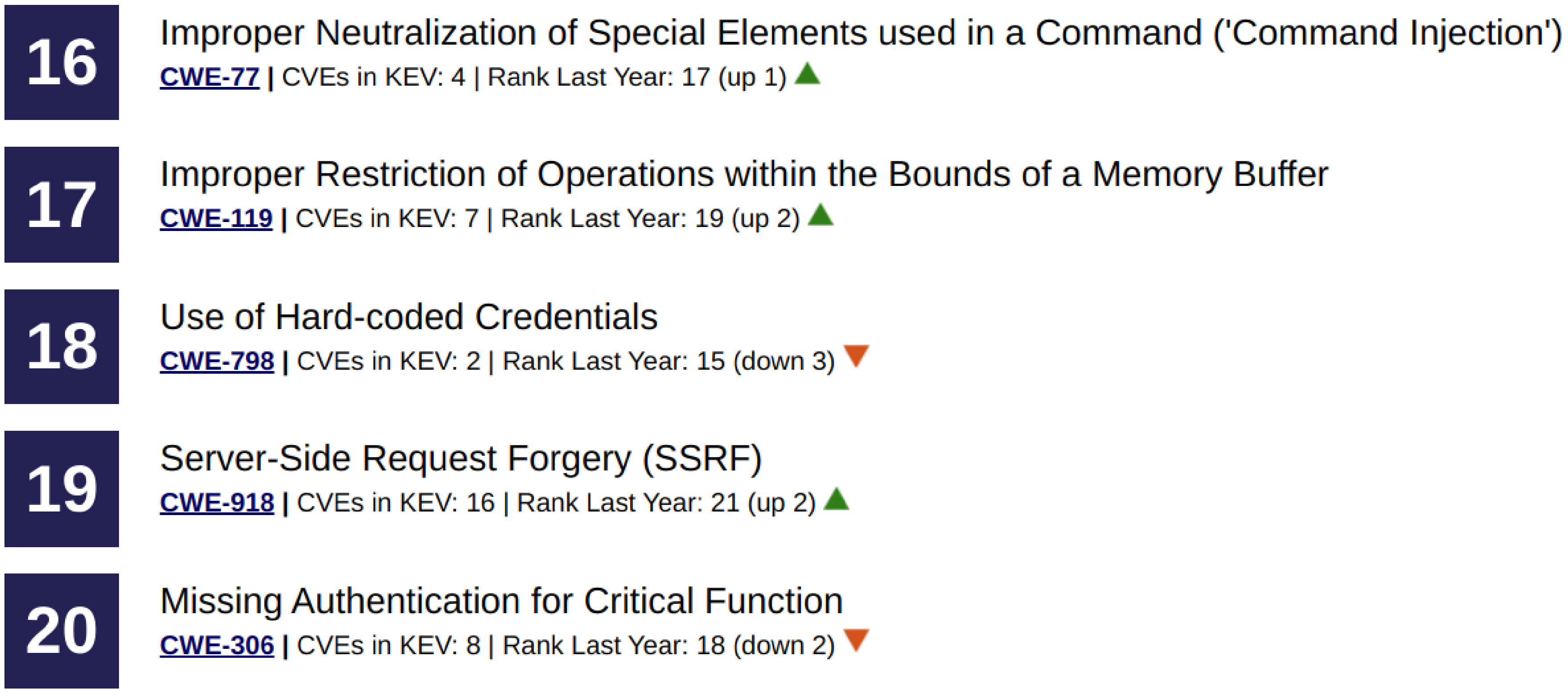
12 NULL Pointer Dereference
CWE-476 | CVEs in KEV: 0 | Rank Last Year: 11 (down 1) ▼

13 Improper Authentication
CWE-287 | CVEs in KEV: 10 | Rank Last Year: 14 (up 1) ▲

14 Integer Overflow or Wraparound
CWE-190 | CVEs in KEV: 4 | Rank Last Year: 13 (down 1) ▼

15 Deserialization of Untrusted Data
CWE-502 | CVEs in KEV: 14 | Rank Last Year: 12 (down 3) ▼

CWE – Top 25 (2023)



16 Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-77 | CVEs in KEV: 4 | Rank Last Year: 17 (up 1) ▲

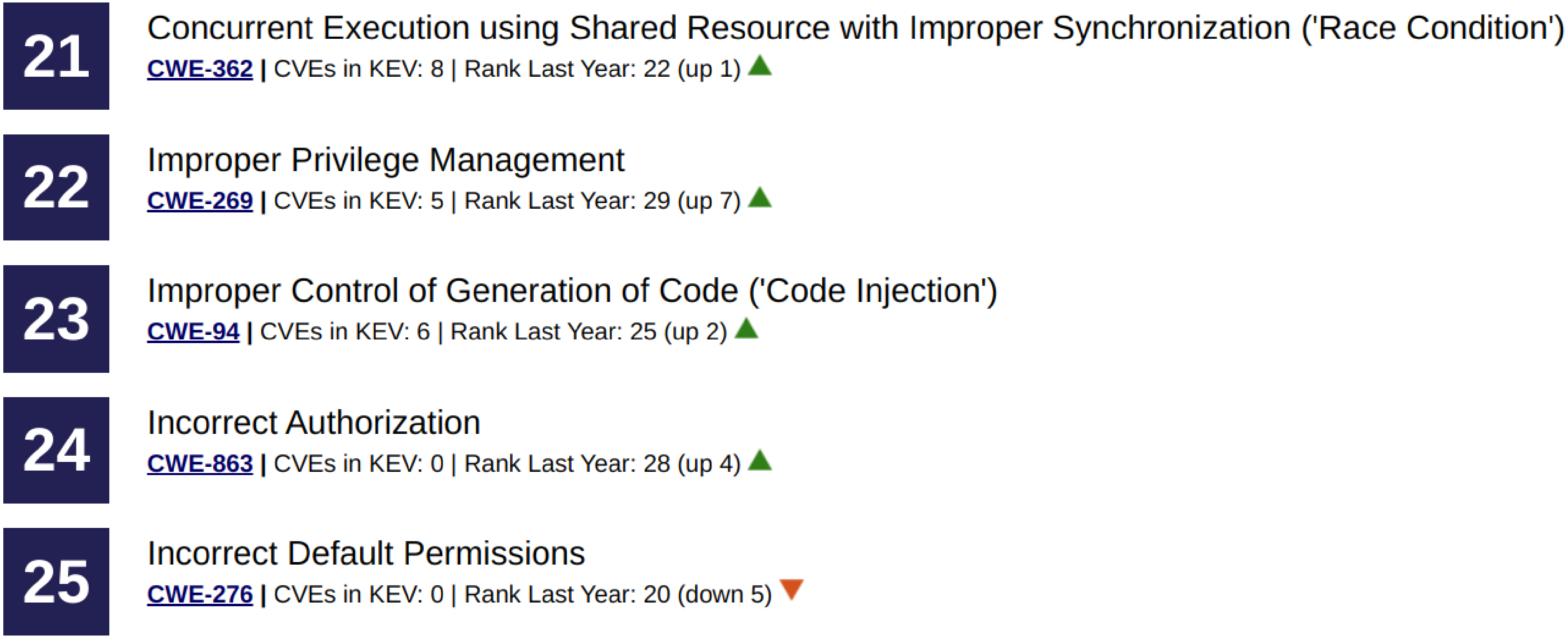
17 Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-119 | CVEs in KEV: 7 | Rank Last Year: 19 (up 2) ▲

18 Use of Hard-coded Credentials
CWE-798 | CVEs in KEV: 2 | Rank Last Year: 15 (down 3) ▼

19 Server-Side Request Forgery (SSRF)
CWE-918 | CVEs in KEV: 16 | Rank Last Year: 21 (up 2) ▲

20 Missing Authentication for Critical Function
CWE-306 | CVEs in KEV: 8 | Rank Last Year: 18 (down 2) ▼

CWE – Top 25 (2023)



21 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-362 | CVEs in KEV: 8 | Rank Last Year: 22 (up 1) ▲

22 Improper Privilege Management
CWE-269 | CVEs in KEV: 5 | Rank Last Year: 29 (up 7) ▲

23 Improper Control of Generation of Code ('Code Injection')
CWE-94 | CVEs in KEV: 6 | Rank Last Year: 25 (up 2) ▲

24 Incorrect Authorization
CWE-863 | CVEs in KEV: 0 | Rank Last Year: 28 (up 4) ▲

25 Incorrect Default Permissions
CWE-276 | CVEs in KEV: 0 | Rank Last Year: 20 (down 5) ▼

Lectura recomendada

Mitre CWE Top 25

https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html

OWASP Top 10

https://owasp.org/www-project-top-ten/