



Criptografía y Seguridad

Vulnerabilidades

¿Que es una vulnerabilidad?



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

Dimensiones de vulnerabilidades

Taxonomia Seven Kingdoms (Tsipenyk)


- Input Validation and Representation
- API Abuse
- Security Features (inexistencia de estas)
- Time and State (estados del sistema inseguros)
- Error Handling
- Code Quality (control de calidad)
- 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: <i>unaffected</i>
Product Android	• affected at 14
	• affected at 13
	• affected at 12L
	• affected at 12
	• affected at 11

Causas raíz: CWE

(Common Weakness Enumeration)

<https://cwe.mitre.org/index.html>

- Taxonomía de amenazas que pueden convertirse en vulnerabilidades
- Es jerárquica, parte de categorías y llega a casos propios de por ejemplo un lenguaje de programación en particular
- Mas de 1000 CWEs
- Una vulnerabilidad se correlaciona con una o mas CWEs

CWE – Top 25 (2023)

1

Out-of-bounds Write

Cuando se escribe antes o despues de un buffer en una zona de memoria.
Afecta disponibilidad y integridad. Muy comun en ASM, C, C++.

[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 Tiene que ver con mezclar codigo y datos sin sanitizar esos datos

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

Usar una seccion de memoria que ya habia sido liberada. Generalmente esto termina en un crasheo del servicio.

[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) ▲

La solucion a esto es no hacer llamados directos al sistema operativo, sino que es mejor usas librerias

CWE – Top 25 (2023)

6

Improper Input Validation

Por ejemplo, pasar un precio negativo me suma dinero a mi cuenta.
Es MUY difícil de detectar

[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')

Le ponemos de nombre a nuestro archivo ../../etc/passwd

[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

Es un problema parecido a XSS. Un atacante explota una funcionalidad del navegador. La idea es que la continuidad entre requests HTTP se obtiene mediante cookies y headers. Cuando yo me logueo a un sitio, empiezo a incluir la cookie que obtuve en mis siguientes requests HTTP. Estas cookies son almacenadas por el navegador. Cuando nosotros cerramos el navegador y lo volvemos a abrir, el navegador puede seguir usando la misma cookie obtenida anteriormente. La idea es que un atacante podría redirigir al cliente a otro sitio (para el cual existe una cookie), utilizando un link que hace una acción que el usuario no quisiera (como por ejemplo hacer /DELETE a los mails del usuario en GMAIL).

El CSRF siempre tiene dos partes, una página atacante y otra página para la cual el usuario ya está logueado (como un home-banking por ejemplo). La página atacante incluye una imagen invisible (de un pixel por ejemplo), Cuando el navegador carga esa imagen, hace un GET a la URL maliciosa, que nos termina obligando a ejecutar algo en la segunda página sin que sepamos.

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 Mecanismo que permite saltarse validaciones

[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) ▼

Esto ocurre en lenguajes que implementan mecanismos de serializacion muy genericos. El problema surge cuando queremos deserializar algo que vino de fuera del sistema. En java, hay clases cuya creacion dispara cambios en el sistema (como las de networking). Entonces, si yo permito deserializar cualquier cosa, me pueden deserializar esas clases y ejecutar codigo arbitrario en el sistema. Los ataques de este tipo terminan en ejecucion remota

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 Es un problema cuando usamos cosas como git, porque la credencial ya no sirve mas

[CWE-798](#) | CVEs in KEV: 2 | Rank Last Year: 15 (down 3) ▼

19

Server-Side Request Forgery (SSRF) Son raros. Puede servir para acceder a servidores internos que no se pueden acceder desde internet.

[CWE-918](#) | CVEs in KEV: 16 | Rank Last Year: 21 (up 2) ▲

20

Missing Authentication for Critical Function Una funcion asume que el usuario ya estaba autenticado

[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) ▲ *Son super dificiles de detectar y arreglar.*
- 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](https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html)

OWASP Top 10

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