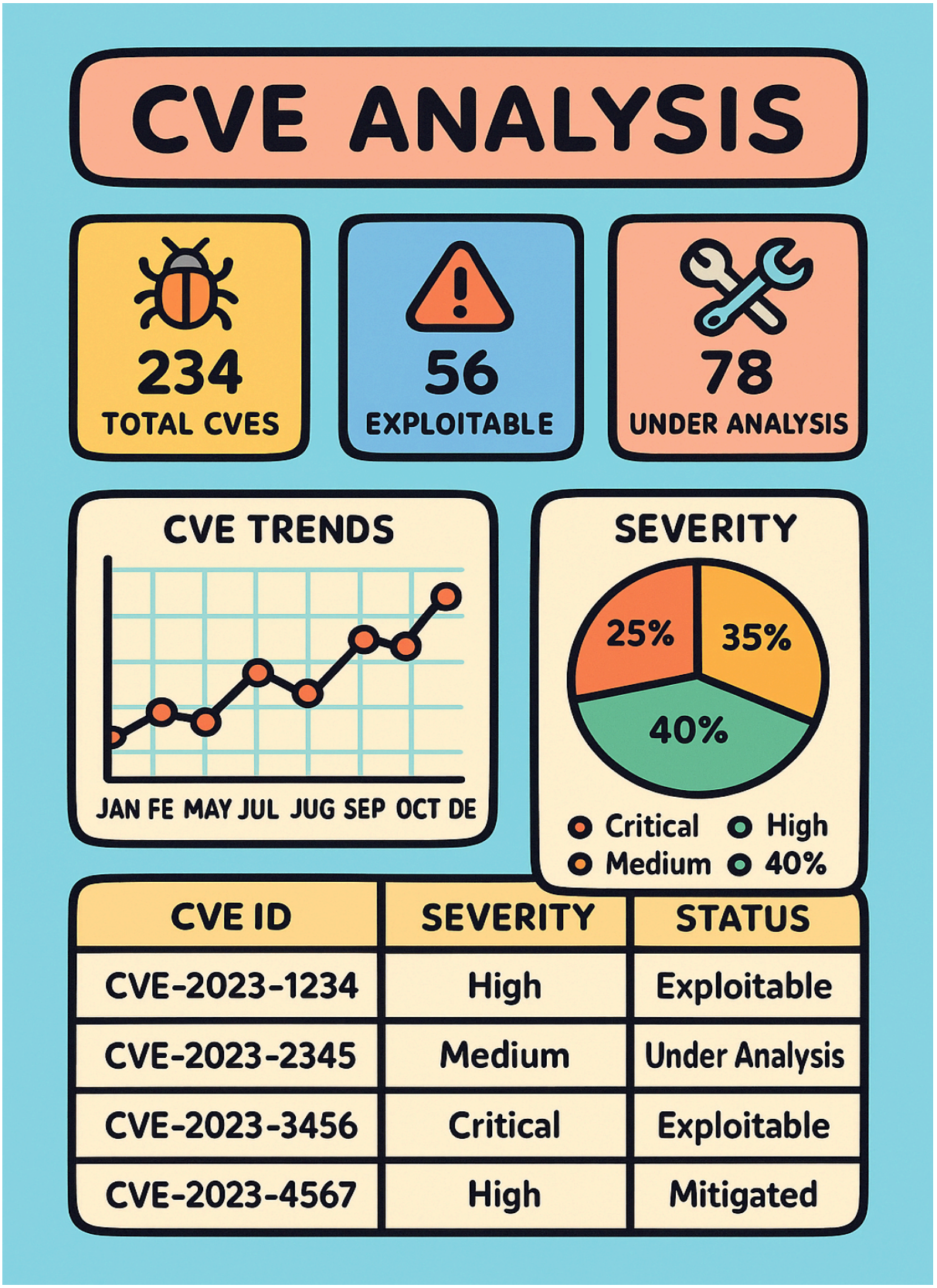
Dashboard Análisis CVEs



CVE ID	SEVERITY	STATUS
CVE-2023-1234	High	Exploitable
CVE-2023-2345	Medium	Under Analysis
CVE-2023-3456	Critical	Exploitable
CVE-2023-4567	High	Mitigated

Juan Miguel Ramírez Pérez - Máster Data & Analytics

Índice

Introducción

El objetivo de este proyecto es analizar las características de los CVEs (Common Vulnerabilities and Exposures) registrados entre 1999 y 2019, para ello se han tomado como fuente varios archivos en formato csv, en concreto cve.csv, vendors.csv, products.csv y vendors_products.csv, procedentes de kraggle.com.

Fuente:
https://www.kaggle.com/datasets/andrewkronser/cve-common-vulnerabilities-and-exposures?resource=download&select=cve.csv

Entre estos datos se encuentran:

- Nombre
- Año de publicación
- Criticidad
- Impacto en confidencialidad, integridad y disponibilidad de los datos
- Breve descripción
- Vía de explotación
- Dificultad de explotación
- Fabricante
- Producto al que pertenece

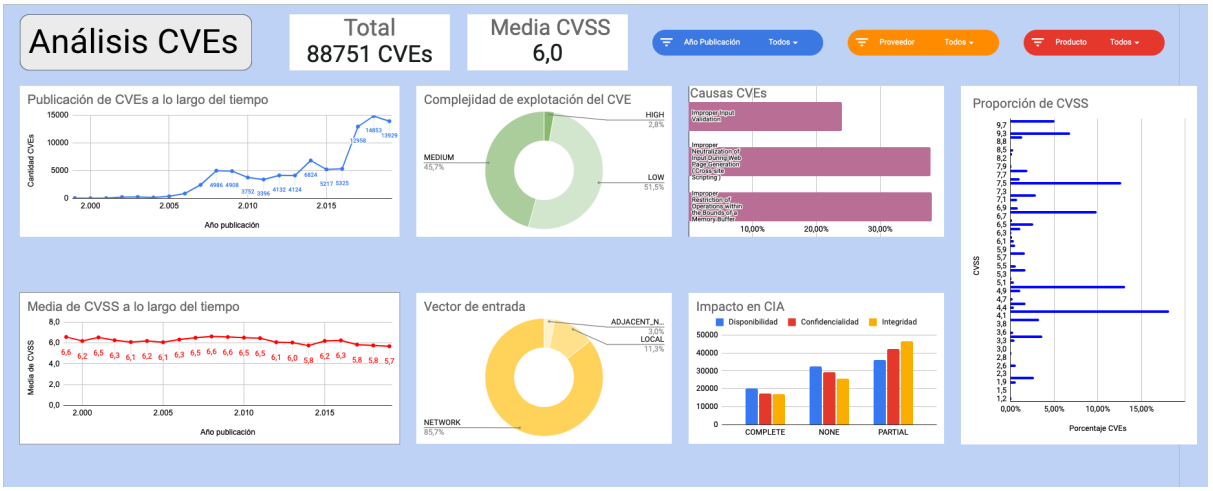
Memoria

A continuación se describen los pasos seguidos durante la ingesta y transformación de los datos en Google Sheets:

1. Descarga de los archivos csv de la fuente mencionada.
2. Importación de datos a Googe Sheets, una hoja por csv.
3. Formateo de columnas, de texto a números y fechas.
4. Importación de columnas products y vendors desde sus hojas a hoja principal "cves".
    a. - Uso de formula =ARRAYFORMULA(BUSCARV()) para mapear registros de productos y proveedores con sus correspondientes CVEs
5. Limpieza de datos
    a. -Varias filas estaban vacías y solo se conocía el nombre del CVE, decido eliminar estos registros para obtener resultados mas óptimos, solo me interesan los CVE de los que tengo información.
    b. -Además, para facilitar el análisis y filtrado de datos añado columnas de año de publicación, cve por cwe, cve por producto y cve por proveedor

Dashboard

A continuación muestro una captura del dashboard final, se puede acceder a él siguiendo el siguiente enlace: https://docs.google.com/spreadsheets/d/1qSyCSUYDR2X4jtc5WZXqRQPMYmEEWwERAEhN65Ym8O8/edit?usp=sharing



Análisis de los resultados

A continuación se realiza un análisis de los resultados observados, respondiendo a las cuestiones planteadas.

Evolución de CVE y su criticidad a lo largo del tiempo

- La publicación de CVEs ha aumentado enormemente a lo largo del tiempo, especialmente a partir de 2015/2016, sin embargo, su criticidad ha ido disminuyendo ligeramente.

Proporción de CVSS (Criticidad)

- La mayor parte de los CVE tienen un CVSS de 4,3 o 5,0, no obstante, el rango en el que más cantidad de CVEs se acumulan entre 6,8 y 10,0.

¿Cual es el mayor vector de entrada para explotar estos CVEs?

Con un 85,7%, el principal vector de entrada es a través de la red

¿Cual es la complejidad de acceso para un atacante?

- Solo el 2,8% de los CVE suponen una complejidad elevada, la mayoría, con un 51,5%, tienen una complejidad baja.

¿Cuáles son los CWE (causas de las vulnerabilidades) más comunes ? (Top 3)

- Validación de entradas incorrecta
- Neutralización incorrecta de entradas durante la generación de paginas web (Cross-site Scripting)
- Restriccion incorrecta de operaciones dentro de los límites de un bufe de memoria

¿Cuál es la proporción de impacto en la CIA (Confidiality, Integrity and Availability) de los datos?

- La mayoría de los CVE suponen un impacto parcial, especialmente para la integridad de los datos.

Cantidad y criticidad de CVEs por producto

- Para tener una visión más clara he filtrado los 10 productos que más CVEs acumulan, siendo el top 3 Android, Chrome y Linux Kernel. El producto con CVEs más críticos es Internet Explorer, seguido de Android y Acrobat DC.

Cantidad y criticidad de CVEs por proveedor

- De nuevo, para mejorar la visibilidad de los datos, filtro los 10 proveedores con mayor cantidad de CVEs.
- El top 5 de proveedores con mayor cantidad de CVEs publicados son Microsoft, IBM, Google, Cisco y Apple.
- El top 5 de proveedores con una media de CVSS más alta son Adobe, Microsoft, Google, Apple y Mozilla.

Hay que tener en cuenta que contar con más CVEs publicados no significa necesariamente que un producto o proveedor sea menos seguro, ya que esto depende en gran parte del volumen de usuarios y de la cantidad de pruebas y análisis a los que se les sometan.