Práctica de laboratorio: Investigar fuentes de información sobre vulnerabilidades

Objetivos

Utilice varias fuentes útiles para investigar más a fondo las vulnerabilidades.

- Parte 1: Investigar vulnerabilidades y exposiciones comunes (CVE)
- Parte 2: Explorar las enumeraciones de debilidades comunes (CWE)
- Parte 3: Investigar los recursos de vulnerabilidades del Instituto Nacional de Estándares y Tecnología (NIST)
- Parte 4: Investigar las vulnerabilidades en el sistema común de puntuación de vulnerabilidades (CVSS)

Aspectos básicos/Situación

En una práctica de laboratorio anterior, encontró varias vulnerabilidades después de escanear un sistema de destino. Ahora utilizará varias fuentes ampliamente disponibles para profundizar en los detalles de las vulnerabilidades. Asignará e investigará las vulnerabilidades en la lista de vulnerabilidades y exposiciones comunes (CVE), la enumeración de debilidades comunes (CWE), la base de datos nacional de vulnerabilidades del NIST y el sistema de puntuación de vulnerabilidades comunes (CVSS).

Recursos necesarios

- Computadora con conexión a Internet

Instrucciones

Parte 1: Investigar vulnerabilidades y exposiciones comunes (CVE)

Paso 1: Explore CVE.

NO TIENE QUE COLOCAR CAPTURAS EN ESTE PASO 1

a. Inicie el sitio web de CVE y vaya a www.cve.org.

b. Lea la descripción general del programa CVE.

1) Seleccione **About > Overview** en el menú.

2) Vea el video de descripción general del programa CVE.

3) Consulte los podcasts disponibles para obtener información más detallada sobre el programa CVE.

¿Cuál es la misión del programa CVE?

Identificar, definir y catalogar las vulnerabilidades de ciberseguridad divulgadas.

¿Quién asigna los ID de CVE?

Las autoridades de numeración de CVE (CNA)

¿Cuáles son los dos objetivos principales del programa CVE?

Escalar el programa para una adopción y cobertura más amplias, y producir más registros CVE más rápidamente (más cerca del tiempo real).

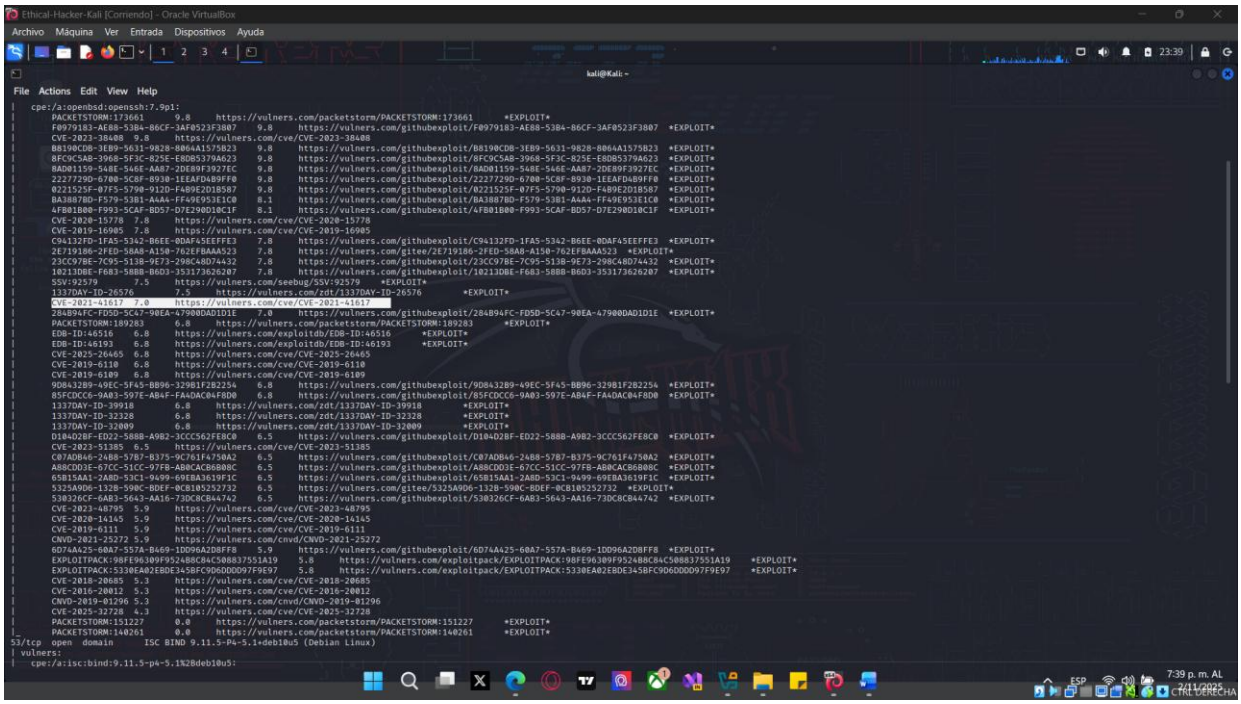
¿Quién opera la CVE?

MITRE Corporation con financiación del Departamento de Seguridad Nacional de EE. UU. (DHS) y el Componente de administración de vulnerabilidades (VMC) de la Agencia de seguridad de infraestructura y ciberseguridad (CISA).

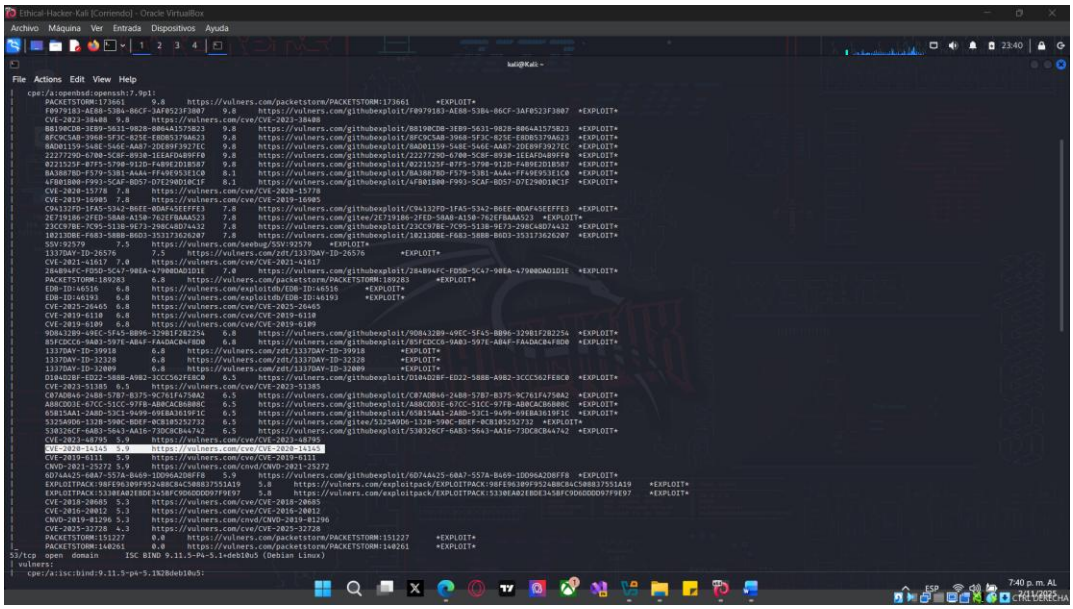
Paso 2: Utilice el programa CVE para recopilar información sobre las vulnerabilidades.

En una práctica de laboratorio anterior, analizó un sistema de destino en busca de vulnerabilidades. La lista de vulnerabilidades encontradas arrojó los siguientes seis CVE:

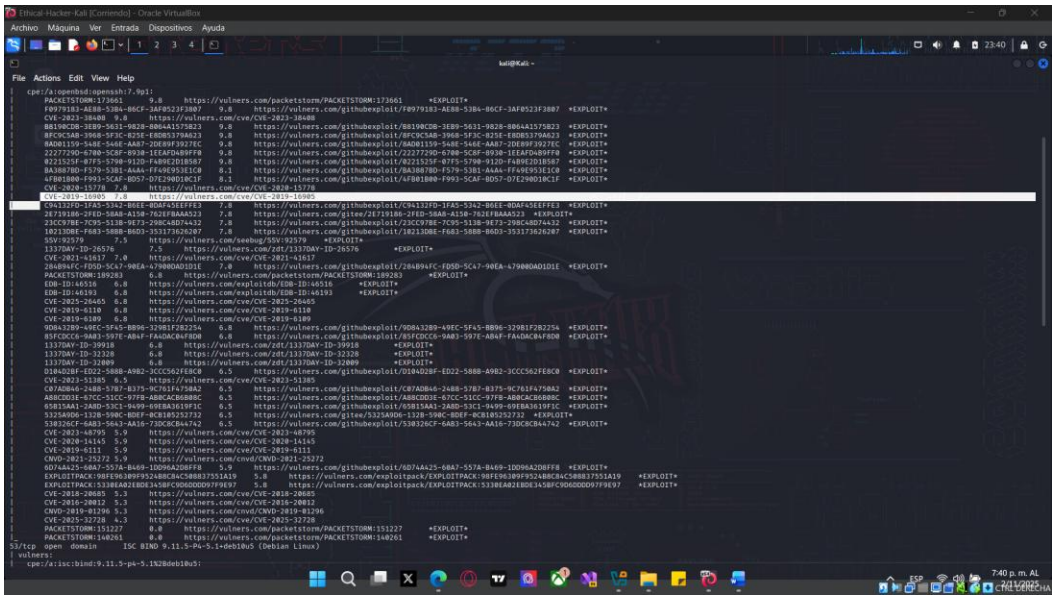
- CVE-2021-41617



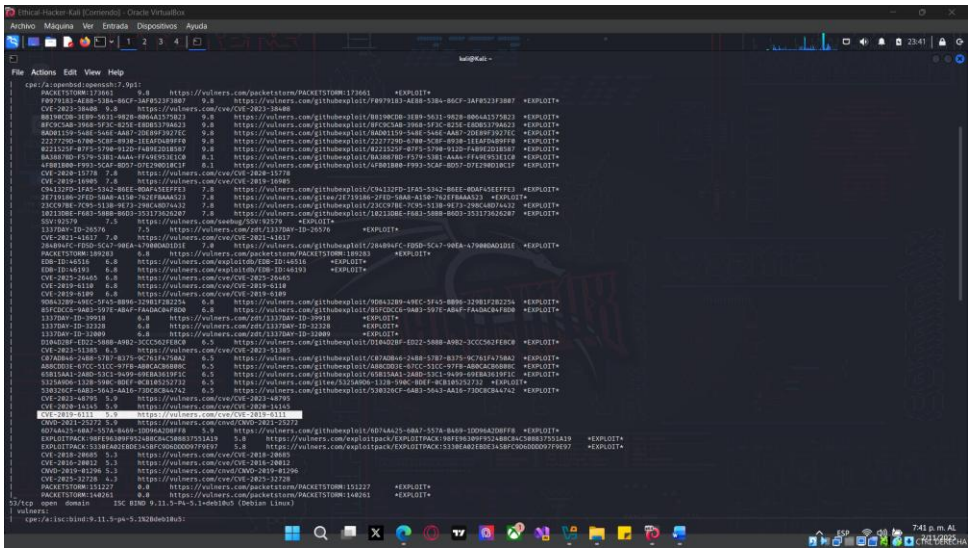
- CVE-2020-14145



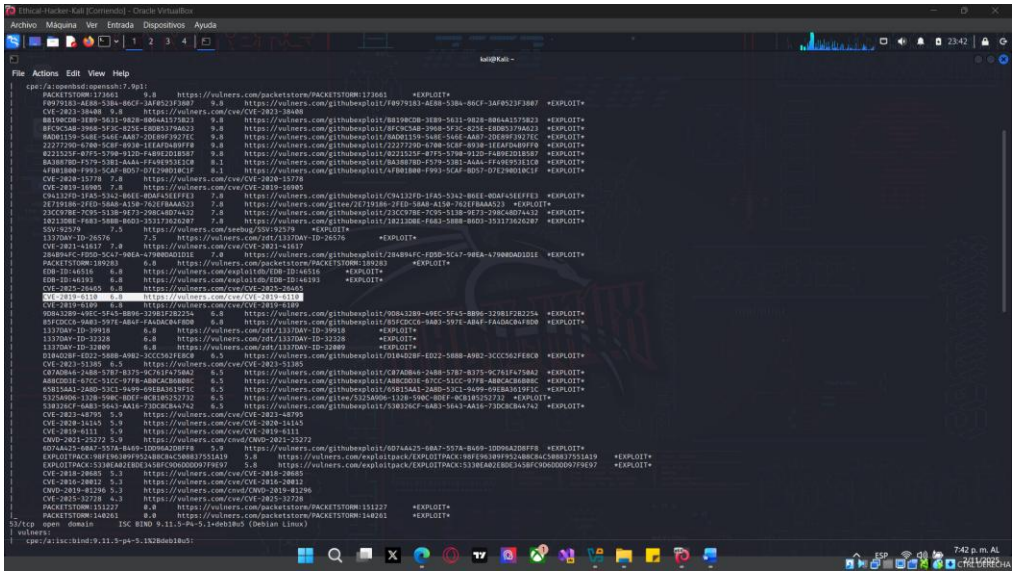
- CVE-2019-16905



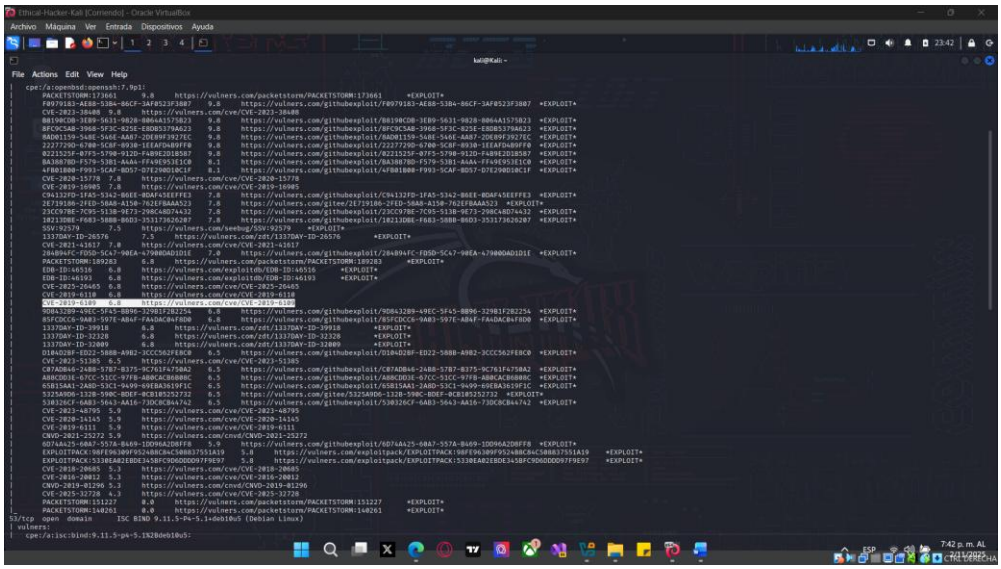
- CVE-2019-6111



- CVE-2019-6110



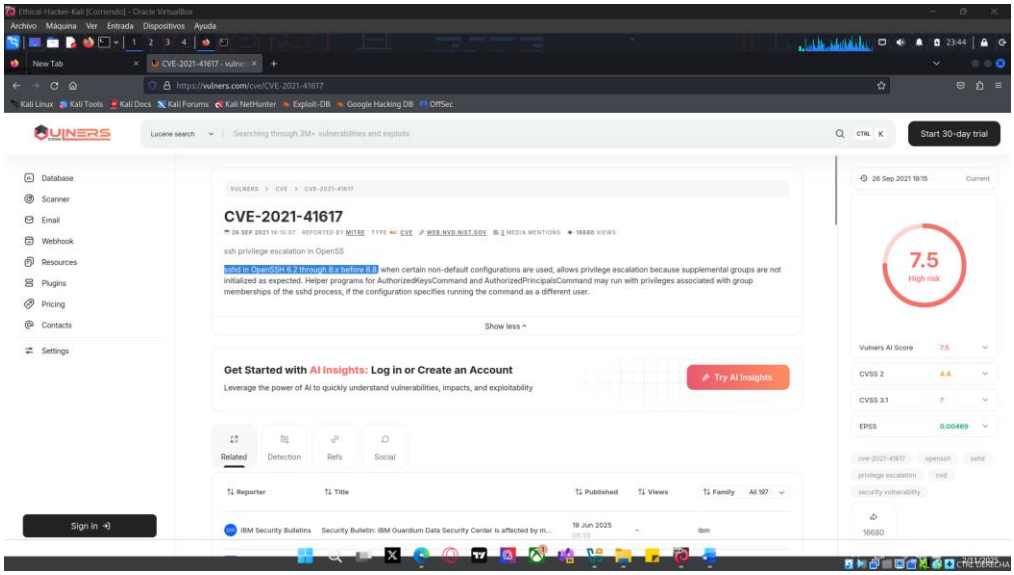
- CVE-2019-6109



COLOCAR CAPTURA DE PANTALLA EN TODOS LOS SIGUIENTES PUNTOS

a. Ingrese la información **CVE-2021-41617 en** la ventana de búsqueda y haga clic en **Find**(Buscar).

¿Qué versiones de OpenSSH están sujetas a esta vulnerabilidad?



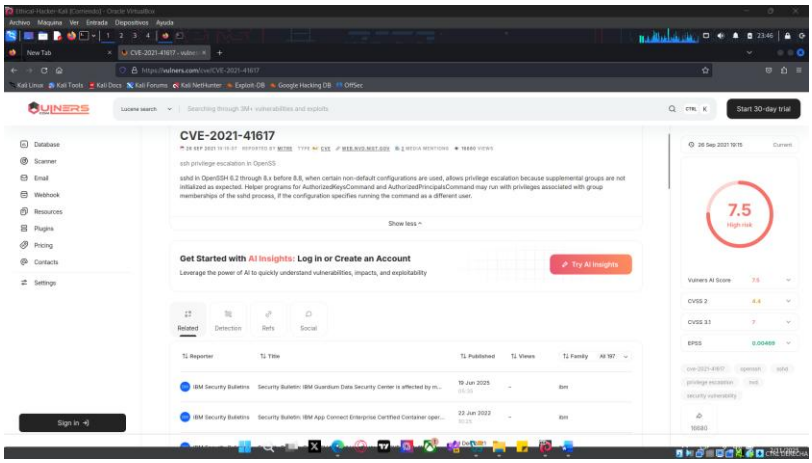
Versiones de la 6.2 a la 8.x, anteriores a la 8.8

¿Cuándo se actualizó por última vez este CVE?

14 de Febrero 2023.

b. En la parte inferior de la página, haga clic en **CVE-2021-41617** para ver información adicional sobre la CVE de la base de datos nacional de vulnerabilidades (NVD) del NIST.

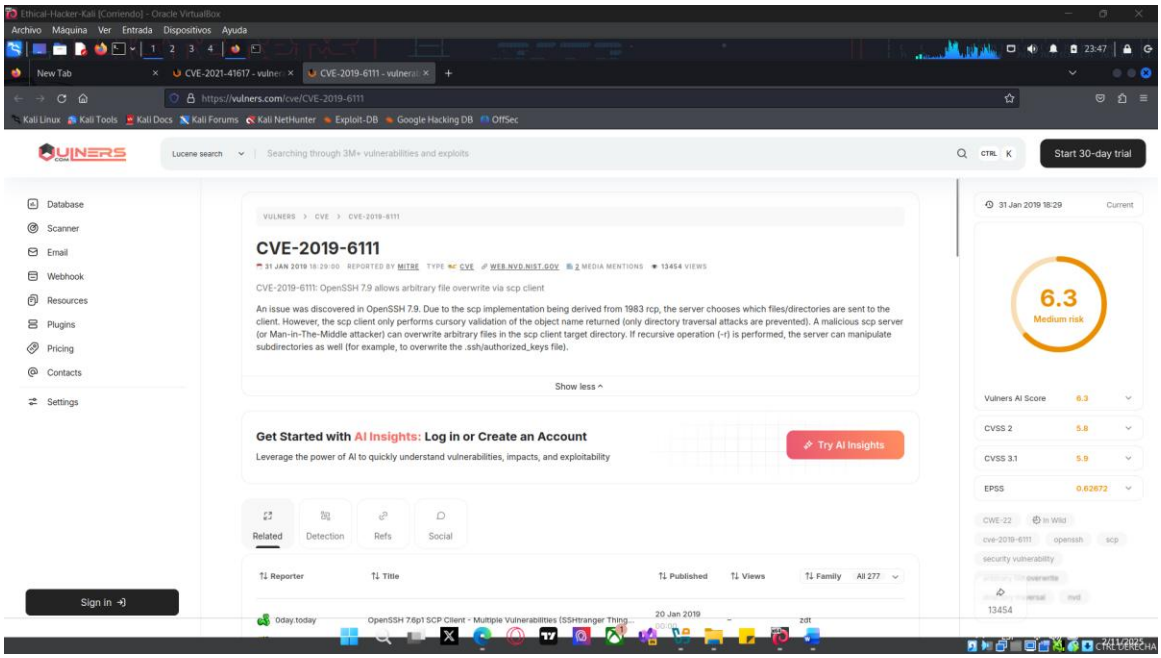
¿Cuál es la puntuación de gravedad de CVSS 3.x para esta CVE?



7.0 ALTO

c. Repita los pasos a y b. para revisar la información de las otras cinco CVE.

¿Cuál de estas CVE implica ataques de intermediario desde un servidor SCP malicioso?



CVE-2019-6111

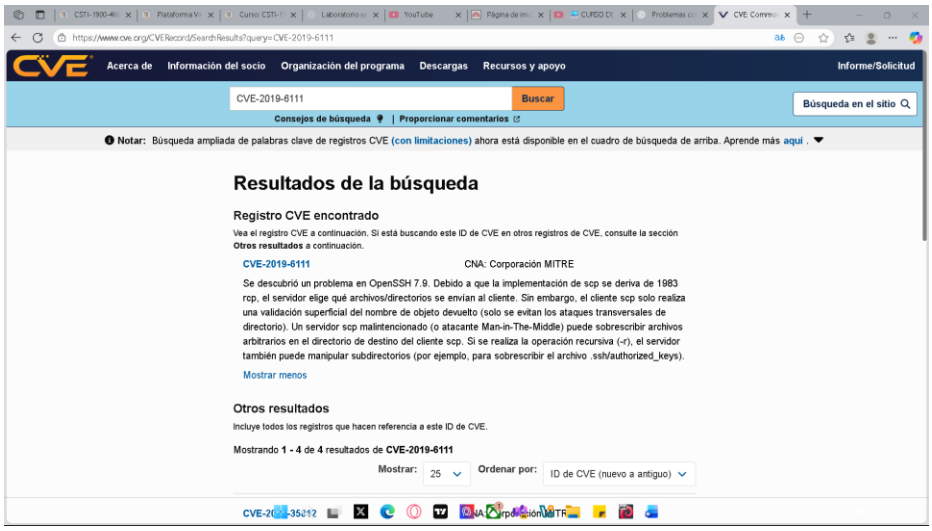
d. En el sitio de CVE (www.cve.org), ingrese **CVE-2019-6111** en el cuadro de búsqueda y haga clic en **Find**(Buscar).

e. Desplácese hasta la parte inferior de la página CVE y haga clic en **CVE-2019-6111** para ver información adicional sobre el NVD.

f. En la página NVD para **CVE-2019-6111**, desplácese hacia abajo hasta la sección **Weakness Enumeration** .

¿Qué ID de CWE está asociado con esta CVE?

CWE-22



Registre esta ID de CWE para usar en la Parte 2.

g. Repita los pasos del a al d. para obtener los ID de CWE asociados con las otras CVE devueltas.

¿Qué CWE están asociadas con cada una de las otras cinco CVE?

CWE-203, CWE-190, CWE-116, CWE-838

CVE-2021-41617 → NVD-CWE-Other (sin mapeo más específico).

CVE-2020-14145 → CWE-203 (*Observable Discrepancy / side-channel*).

CVE-2019-16905 → CWE-190 (*Integer Overflow or Wraparound*).

CVE-2019-6110 → CWE-838 (*Argument Injection or Modification*).

CVE-2019-6109 → CWE-116 (*Improper Encoding or Escaping of Output*).

Registre estas ID de CWE para usarlas en la Parte 2.

Parte 2: Investigar los recursos de vulnerabilidades del Instituto Nacional de Estándares y Tecnología (NIST)

Paso 1: Explore NIST.

a. Inicie el sitio web de NIST navegando a https://www.nist.gov.

b. Seleccione **About NIST** > **About Us** en el menú y revise la descripción general de NIST.

¿Cuál es la misión de NIST?

“Promover la innovación y la competitividad industrial de los Estados Unidos a través del avance de la ciencia, los estándares y la tecnología para mejorar la seguridad económica y la calidad de vida”.

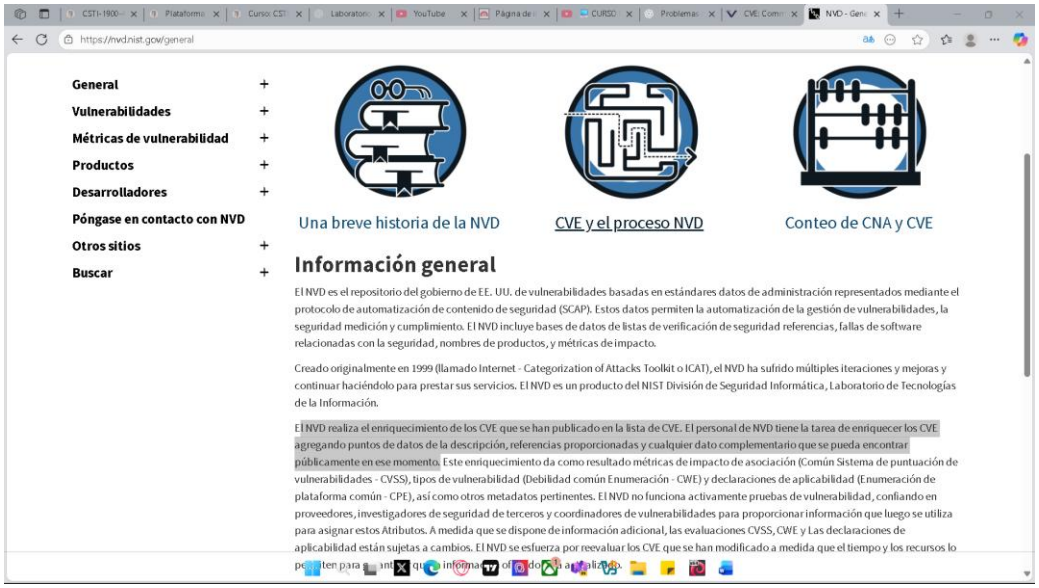
c. Explore la base de datos nacional de vulnerabilidad (NVD)

1) Regrese a la página de inicio de NIST y seleccione **Topics** > **Information Technology** en el menú.

2) Seleccione **National Vulnerability Database** en la lista **Featured Content** .

3) Haga clic en **General** para ver y revisar la Información general sobre el NVD.

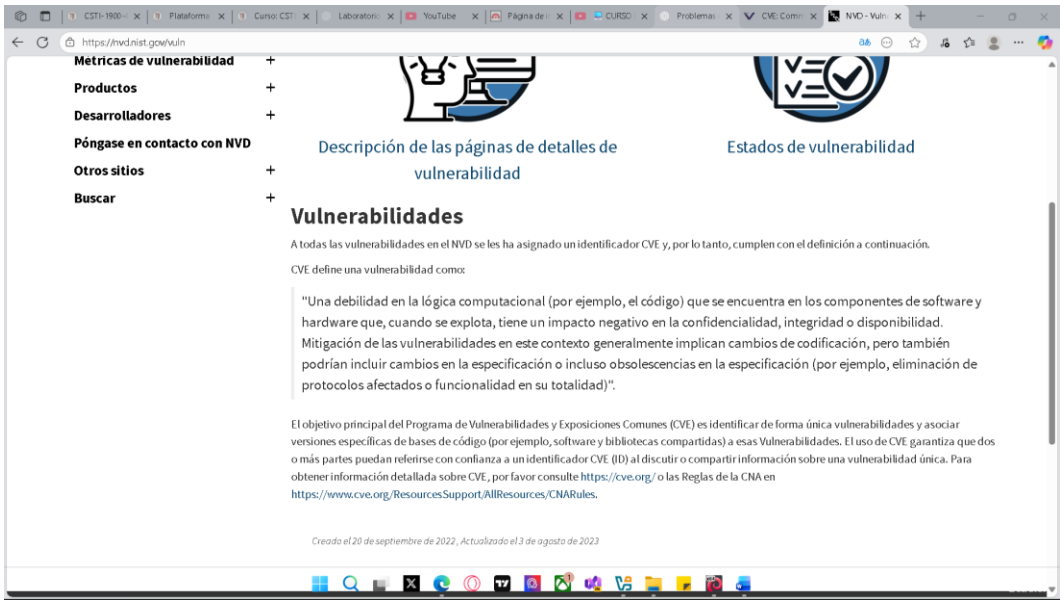
¿Cuál es la relación entre NVD y CVE?



El NVD realiza un escaneo de las CVE publicadas en el diccionario de CVE. El personal de NVD analiza las CVE y proporciona detalles adicionales.

4) Expanda el menú en **General** y haga clic en **NVD Dashboard**.

¿Cuántas vulnerabilidades de CVE contiene el NVD?



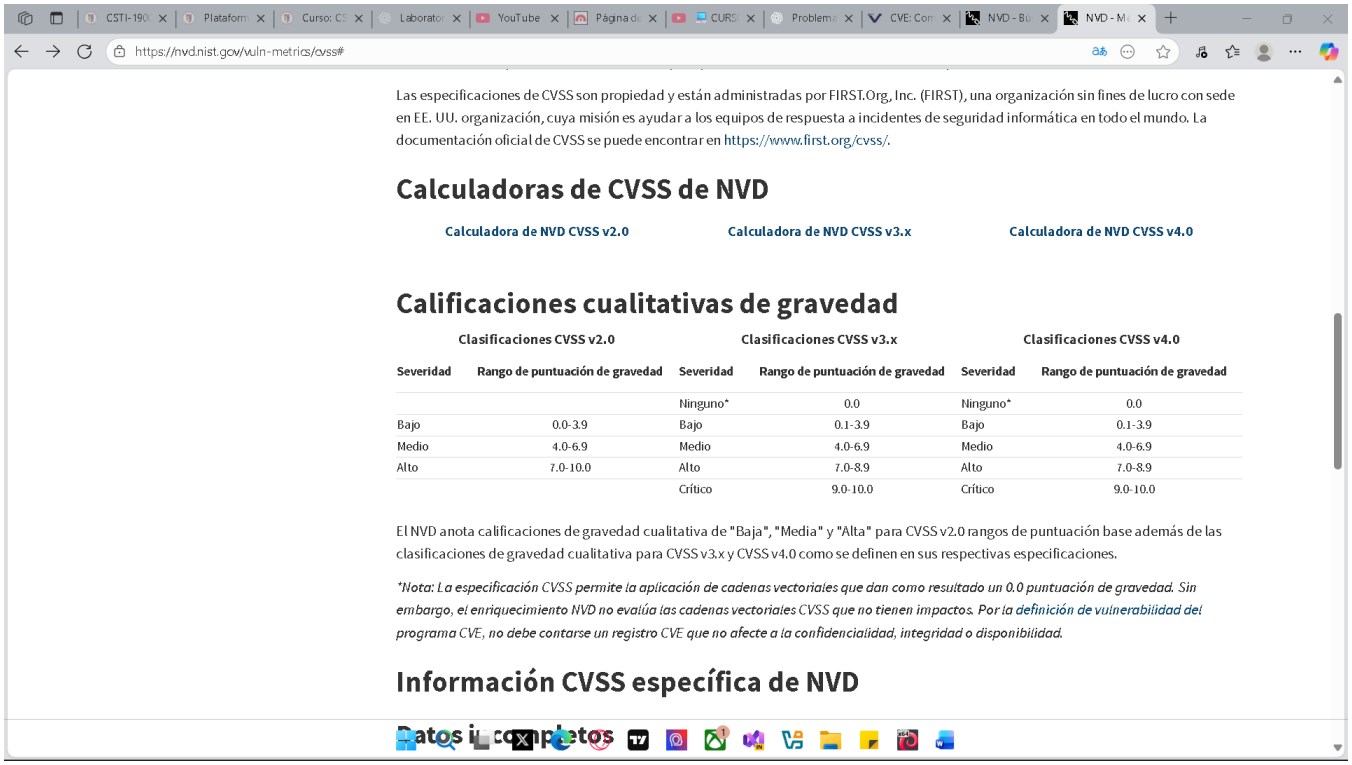
La respuesta varía. En el momento de escribir este curso: 211116

¿Cuál es la vulnerabilidad puntuada más reciente y cuál es la calificación CVSS?

La respuesta variará, pero al momento de redactar este curso: CVE-2023-20990 con una gravedad CVSS de 4,4 MEDIA

5) Vuelva a la página de la base de datos nacional de vulnerabilidades https://nvd.nist.gov/.
6) Haga clic en **Vulnerability Metrics** en el menú a la izquierda de la página.

¿Qué método se utiliza para medir cualitativamente la gravedad de las vulnerabilidades?



https://nvd.nist.gov/vuln-metrics/cvss#

Las especificaciones de CVSS son propiedad y están administradas por FIRST.Org, Inc. (FIRST), una organización sin fines de lucro con sede en EE. UU. organización, cuya misión es ayudar a los equipos de respuesta a incidentes de seguridad informática en todo el mundo. La documentación oficial de CVSS se puede encontrar en https://www.first.org/cvss/.

Calculadoras de CVSS de NVD

Calculadora de NVD CVSS v2.0 | Calculadora de NVD CVSS v3.x | Calculadora de NVD CVSS v4.0

Calificaciones cualitativas de gravedad

Clasificaciones CVSS v2.0		Clasificaciones CVSS v3.x		Clasificaciones CVSS v4.0	
Severidad	**Rango de puntuación de gravedad**	**Severidad**	**Rango de puntuación de gravedad**	**Severidad**	**Rango de puntuación de gravedad**
		Ninguno*	0.0	Ninguno*	0.0
Bajo	0.0-3.9	Bajo	0.1-3.9	Bajo	0.1-3.9
Medio	4.0-6.9	Medio	4.0-6.9	Medio	4.0-6.9
Alto	7.0-10.0	Alto	7.0-8.9	Alto	7.0-8.9
		Crítico	9.0-10.0	Crítico	9.0-10.0

El NVD anota calificaciones de gravedad cualitativa de "Baja", "Media" y "Alta" para CVSS v2.0 rangos de puntuación base además de las clasificaciones de gravedad cualitativa para CVSS v3.x y CVSS v4.0 como se definen en sus respectivas especificaciones.

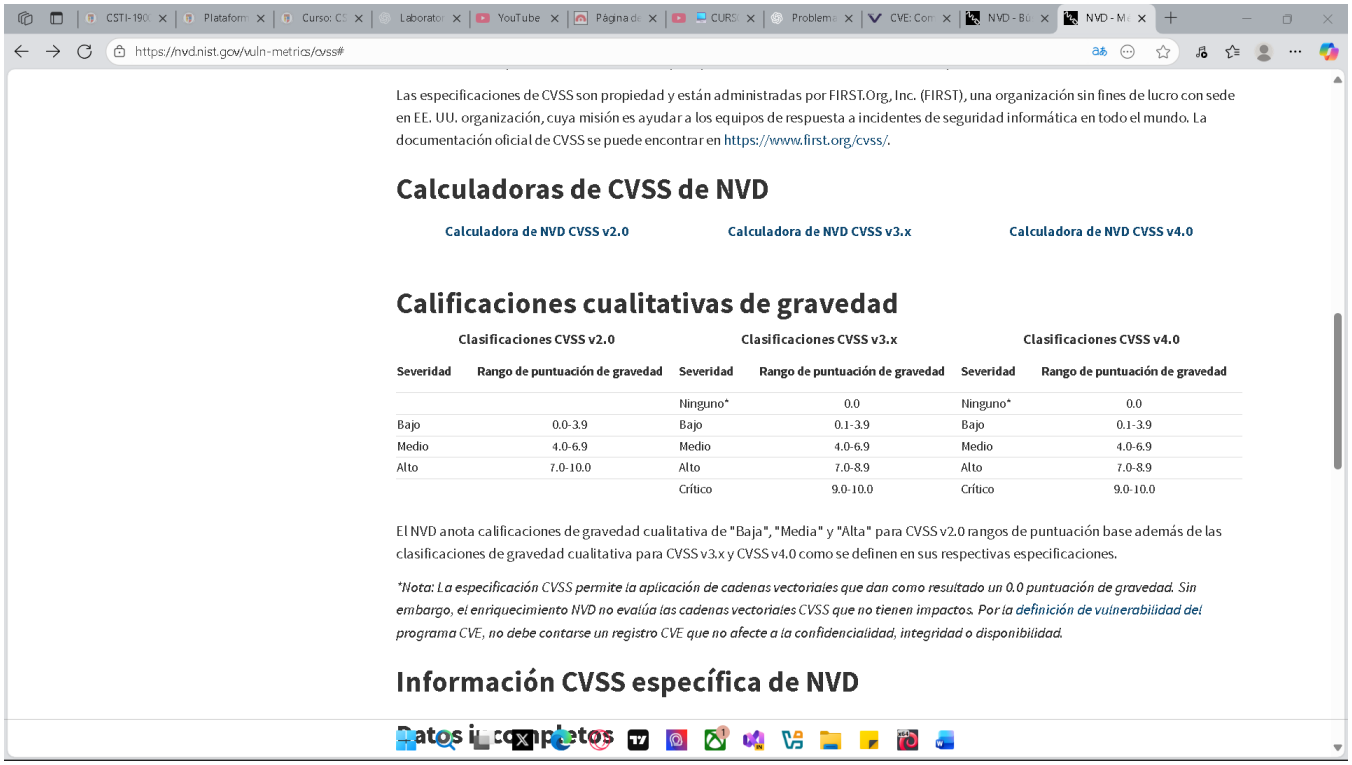
**Nota: La especificación CVSS permite la aplicación de cadenas vectoriales que dan como resultado un 0.0 puntuación de gravedad. Sin embargo, el enriquecimiento NVD no evalúa las cadenas vectoriales CVSS que no tienen impactos. Por la definición de vulnerabilidad del programa CVE, no debe contarse un registro CVE que no afecte a la confidencialidad, integridad o disponibilidad.*

Información CVSS específica de NVD

Datos incompletos

Sistema de puntuación de vulnerabilidades comunes (CVSS)

¿Cuántas clasificaciones de gravedad tiene CVSS v3.0 y cuáles son?



https://nvd.nist.gov/vuln-metrics/cvss#

Las especificaciones de CVSS son propiedad y están administradas por FIRST.Org, Inc. (FIRST), una organización sin fines de lucro con sede en EE. UU. organización, cuya misión es ayudar a los equipos de respuesta a incidentes de seguridad informática en todo el mundo. La documentación oficial de CVSS se puede encontrar en https://www.first.org/cvss/.

Calculadoras de CVSS de NVD

Calculadora de NVD CVSS v2.0 | Calculadora de NVD CVSS v3.x | Calculadora de NVD CVSS v4.0

Calificaciones cualitativas de gravedad

Clasificaciones CVSS v2.0		Clasificaciones CVSS v3.x		Clasificaciones CVSS v4.0	
Severidad	**Rango de puntuación de gravedad**	**Severidad**	**Rango de puntuación de gravedad**	**Severidad**	**Rango de puntuación de gravedad**
		Ninguno*	0.0	Ninguno*	0.0
Bajo	0.0-3.9	Bajo	0.1-3.9	Bajo	0.1-3.9
Medio	4.0-6.9	Medio	4.0-6.9	Medio	4.0-6.9
Alto	7.0-10.0	Alto	7.0-8.9	Alto	7.0-8.9
		Crítico	9.0-10.0	Crítico	9.0-10.0

El NVD anota calificaciones de gravedad cualitativa de "Baja", "Media" y "Alta" para CVSS v2.0 rangos de puntuación base además de las clasificaciones de gravedad cualitativa para CVSS v3.x y CVSS v4.0 como se definen en sus respectivas especificaciones.

**Nota: La especificación CVSS permite la aplicación de cadenas vectoriales que dan como resultado un 0.0 puntuación de gravedad. Sin embargo, el enriquecimiento NVD no evalúa las cadenas vectoriales CVSS que no tienen impactos. Por la definición de vulnerabilidad del programa CVE, no debe contarse un registro CVE que no afecte a la confidencialidad, integridad o disponibilidad.*

Información CVSS específica de NVD

Datos incompletos

Cinco. Son: Ninguna, Baja, Media, Alta y Crítica.

Reflexión

¿Cuál es la relación entre CVE, CWE, NVD y CVSS?

CVE identifica las vulnerabilidades,
CWE clasifica la causa o tipo de debilidad,
NVD amplía la información de las CVE con detalles y análisis,
y CVSS mide la gravedad de cada vulnerabilidad.

CVE enumera las vulnerabilidades que se han descubierto, CWE las clasifica, NVD proporciona detalles y CVSS proporciona calificaciones de gravedad.