



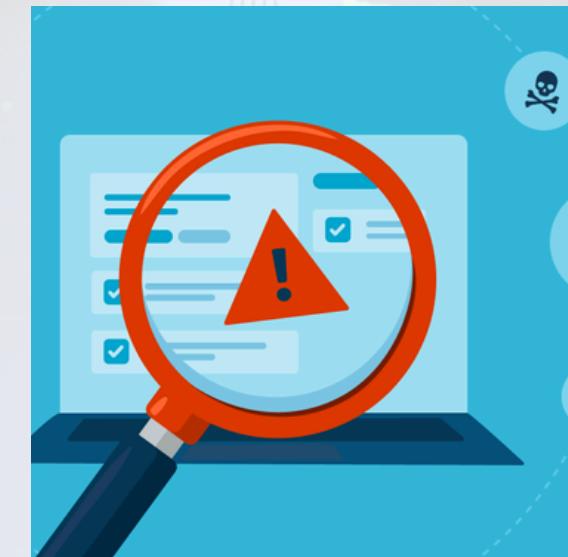
Cybersecurity Consulting

GRUPO 3

Introducción

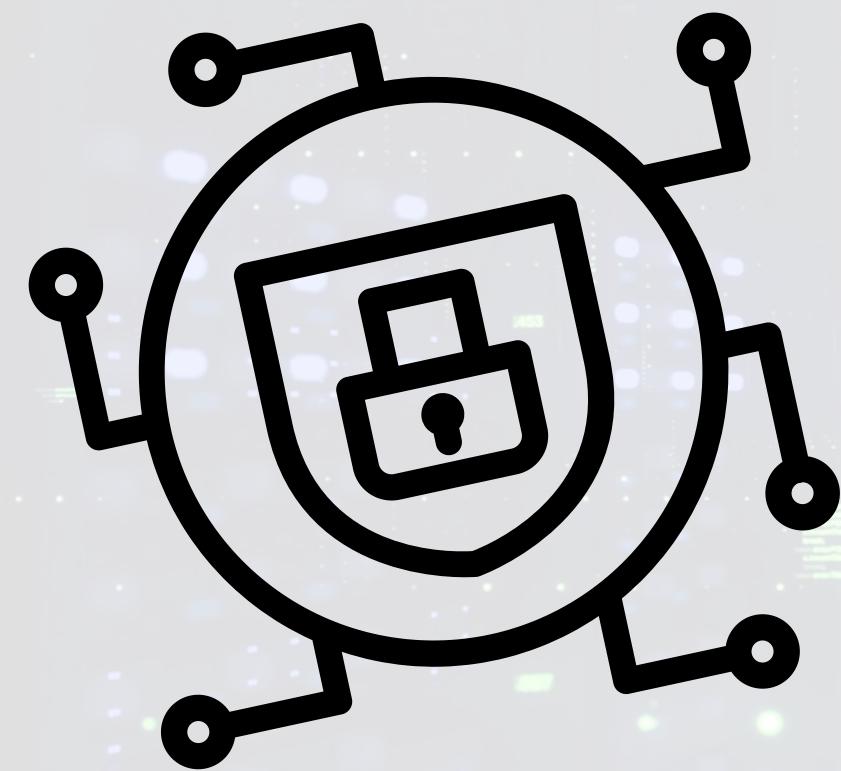
Una empresa llamada TrustShield Financial nos contrata para que hagamos una análisis de su estructura en busca de vulnerabilidades

Nuestro equipo se ha focalizado en las vulnerabilidades de las aplicaciones web de la empresa



Las categorías escogidas han sido elegidas por su numero de incidentes durante los últimos años





Categorías de vulnerabilidades



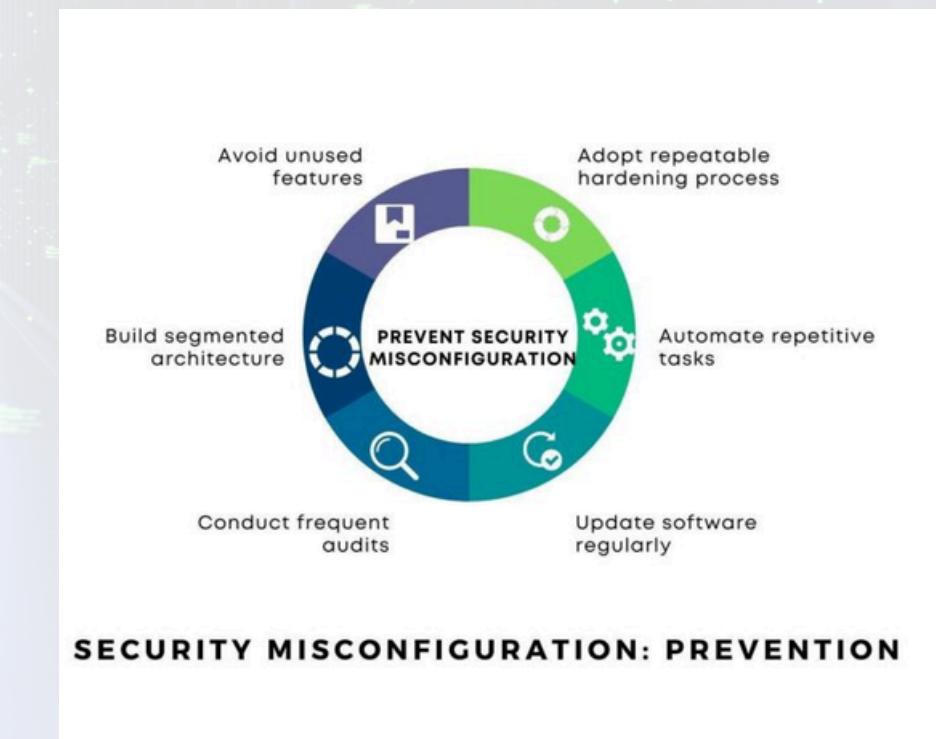
Security Misconfiguration

Descripción

90% de los sistemas testados tienen esta falla.

Consecuencia de un alto nivel de configuración.

- Falta de un Bastionado robusto
- Funciones habilitadas innecesarias
- Cuentas con contraseñas por defecto.
- Manejo de errores inadecuado.
- Sistemas sin ultimas actualizaciones de seguridad.
- Configuración de seguridad con valores no seguros.
- Software vulnerable.



CVE



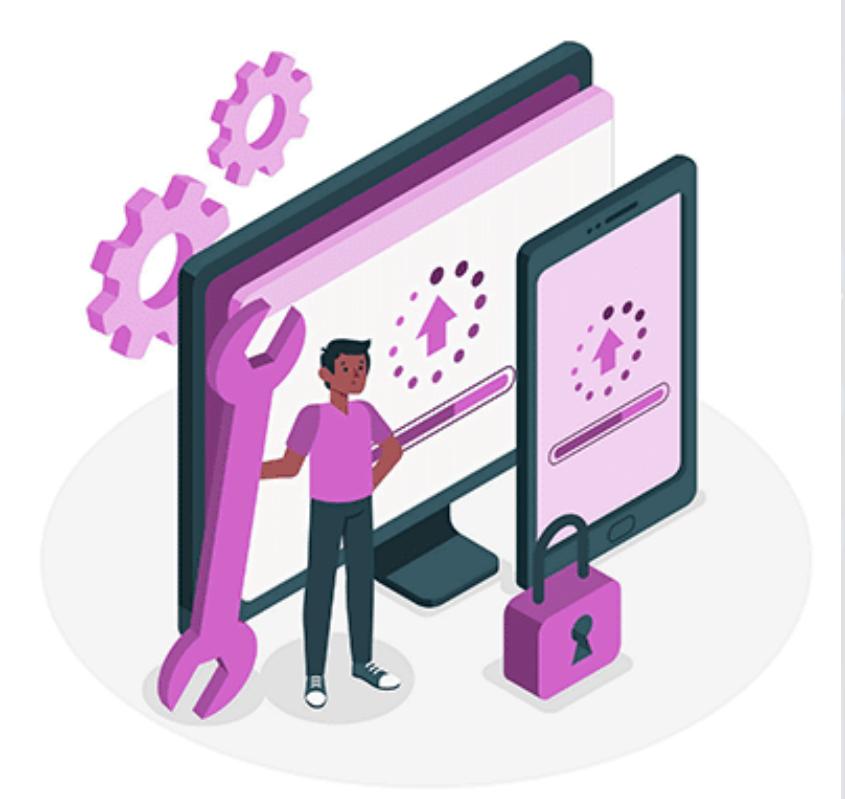
**CVE-2024-
35933**

El kernel de linux tiene un error en dispositivos intel con su Bluetooth con la función btintel_read_version creando fallos en el sistema.

GRAVEDAD: MEDIO
PUNTUACIÓN: 5.5

CONTRAMEDIDAS

- Evitar utilizar elementos innecesarios.
- Establecer tareas rutinarias que revisen cambios de seguridad.
- Segmentar la arquitectura utilizando contenedores.
- Enviar directivas de seguridad a los clientes.





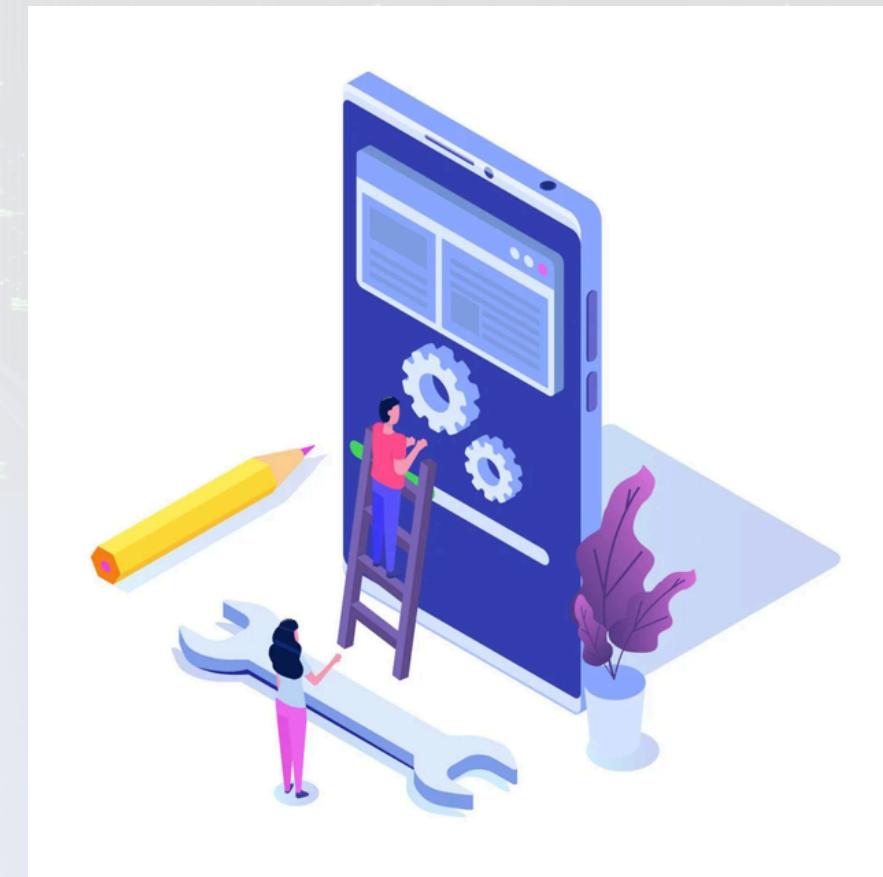
Vulnerable and Outdated Components

Descripción

Uso de componentes no actualizados o descontinuados.

Falta de atención en el mantenimiento de los componentes.

- Desconocimiento de las versiones utilizadas.
- Utilizar un software vulnerable, sin soporte o desactualizado.
- No escanear frecuentemente por vulnerabilidades.
- Utilización de componentes no compatibles entre si.
- Utilizar una configuración errónea en nuestros componentes.



CVE



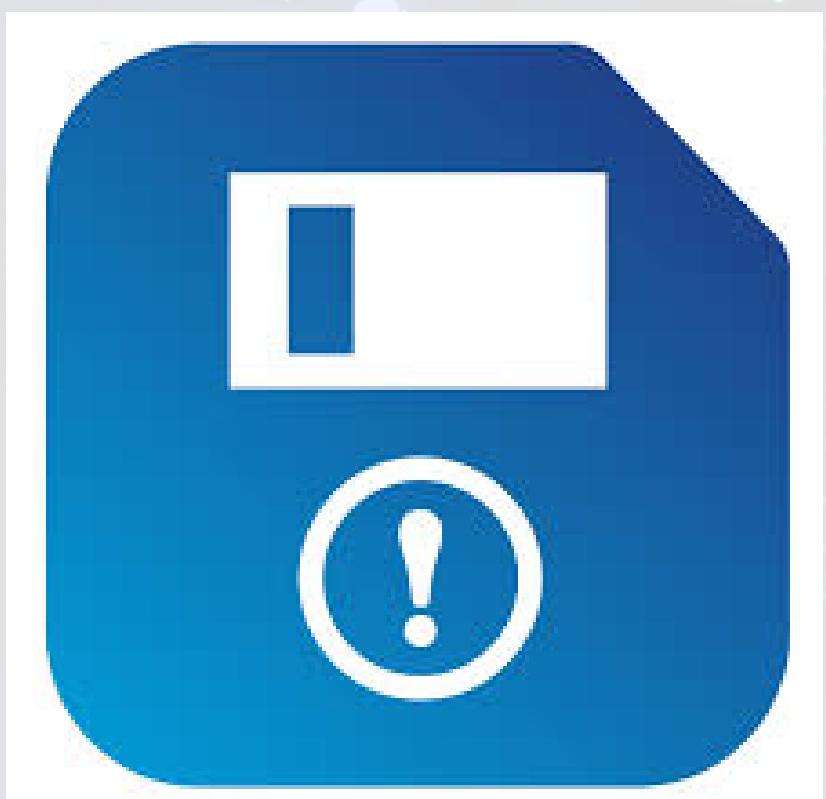
CVE-2022-
24740

En versiones concretas de Volto, un atacante podía intercambiar cookies de autenticación para ganar control en la cuenta del usuario.

GRAVEDAD: ALTO
PUNTUACIÓN: 7.5

CONTRAMEDIDAS

- Eliminar elementos en desuso.
- Comprobar frecuentemente las versiones.
- Revisar de forma frecuente el Common Vulnerability and Exposures(CVE)
- Obtener los componentes de fuentes seguras.





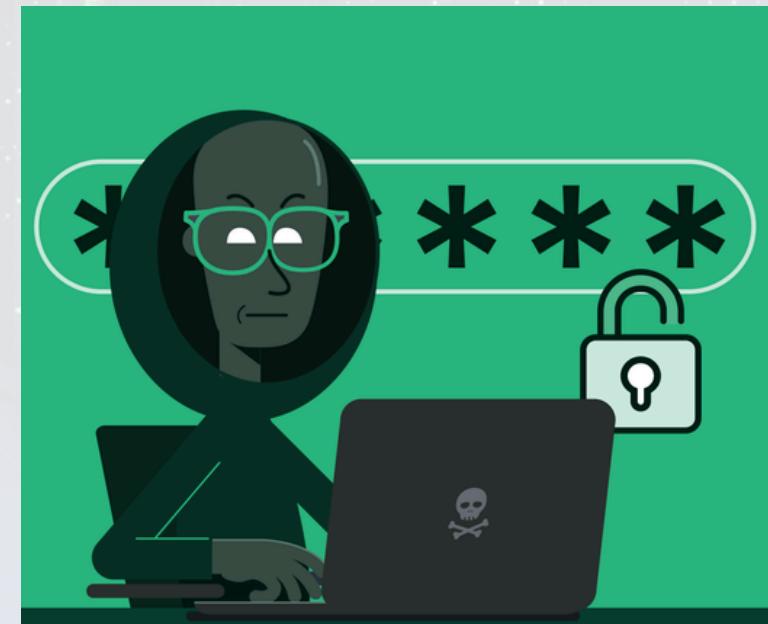
Broken Access Control

Descripción

- Compartir información.
- Usuarios no autorizados.

Alguna de las vulnerabilidades más comunes:

- Acceso y modificación de la cuenta de otra persona.
- Elevación de privilegios.
- Forzar navegación a páginas autenticadas.



CVE



CVE-2024-4263

Con pocos permisos podemos borrar. Para solucionarlo tenemos que actualizar a la versión 2.10.1 o superior.

GRAVEDAD: MEDIA
PUNTUACIÓN: 5.4

CONTRAMEDIDAS

- Registrar fallos y comunicación.
- Controles de acceso a niveles de datos.
- Limitar tasa de acceso permitido a las APIs y controladores.





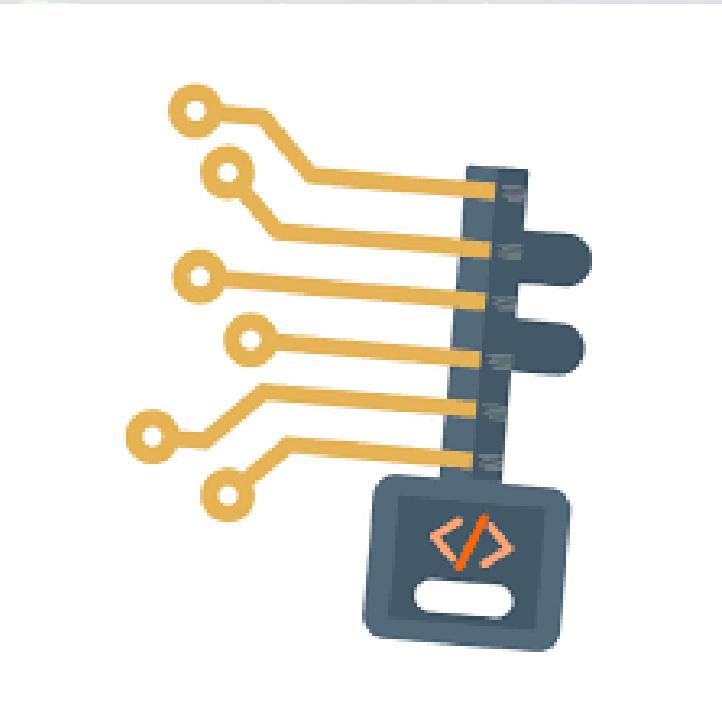
Cryptographic Failures

Descripción

- Mirar datos confidenciales.
- Protección adicional.

Algunas de las vulnerabilidades más comunes:

- Utilización de algoritmos criptográficos antiguos.
- Funciones hash obsoletas.
- Se incluyen claves criptográficas en repositorios.



CVE



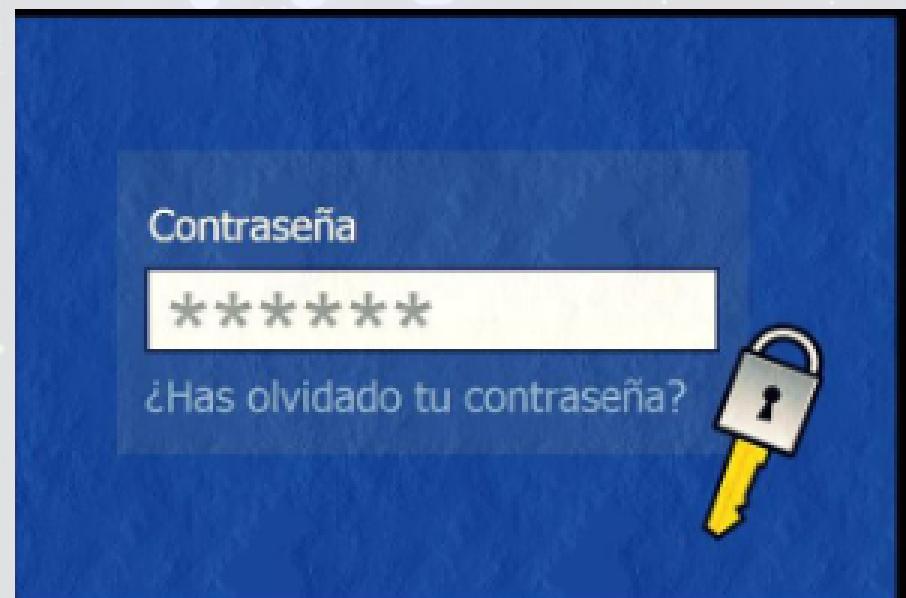
CVE-2024-
45402

La falla podría conducir a un escenario de uso después de la liberación lo que permitiría la ejecución arbitraria del código. Para solucionarlo tenemos que actualizar la versión.

GRAVEDAD: ALTA
PUNTUACIÓN: 8.6

CONTRAMEDIDAS

- Asegurarse de cifrar todos los datos sensibles.
- No almacenar datos sensibles innecesariamente.
- Clasificar datos identificando si son confidenciales con respecto la ley de privacidad.



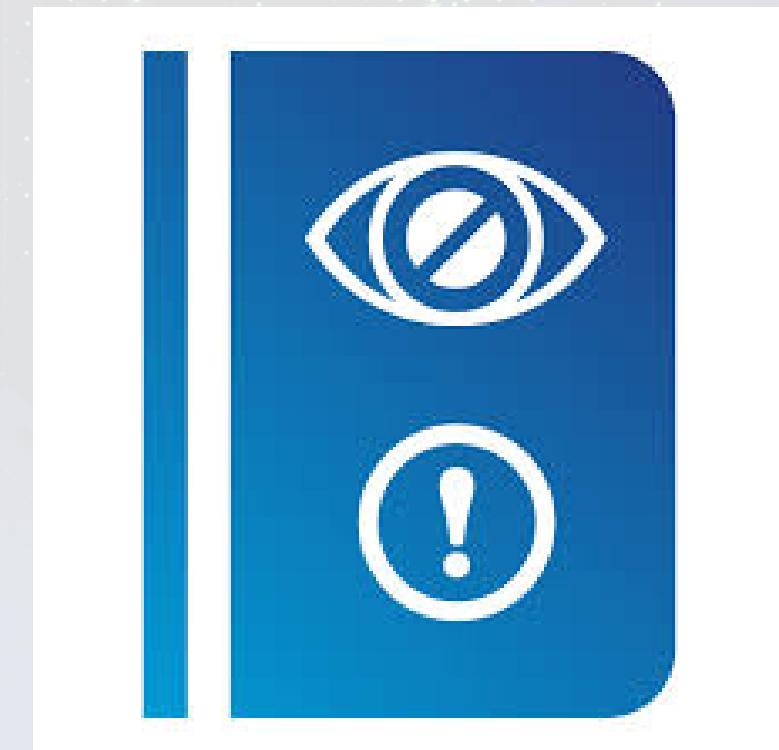


Security logging and monitoring failures

Descripción

Si no se monitorizan las actividades de manera correcta nos costará más responder a un ataque. Esto ocurre si:

- Los eventos con autor no quedan registrados.
- Los avisos y errores no quedan registrados.
- No se monitorizan los logs.
- Sin copias de seguridad de los logs.
- No hay procesos de escala de respuesta.
- Los pentesting no generan alertas



CONTRAMEDIDAS

Podremos solventar esta vulnerabilidad de las siguientes formas:

- Registrar los logins.
- Logs en formato legible para gestores.
- Logs codificados.
- Seguimiento de auditoría para acciones importantes.
- DevSecOps.
- Plan de respuesta y recuperación a incidentes.

Logging & Monitoring





Server-side request forgery (SSRF)

Descripción

Permite a un atacante enviar una solicitud a la red interna a través de una consulta HTTP a la aplicación web.



CVE



CVE-2021- 21973

Plugin de VMware vCenter
Server que no valida
correctamente las URLs. Ya
 parcheada.

GRAVEDAD: MEDIA
PUNTUACIÓN: 5.3

CONTRAMEDIDAS

Desde la capa de red:

- Separar el acceso remoto en distintas redes.
- Deny by default en el firewall.

Desde la capa de aplicación:

- Validar input del usuario.
- Deshabilitar redirecciones HTTP.
- Validar la información dirigida al cliente.





Insecure Design

Descripción

Falla en la etapa de diseño de un sistema o software. Se suele confundir con una implementación insegura aunque no se refieren a lo mismo.



CVEs



CVE-2022-
44004

Problema en BLAKCLICK
donde los atacantes
podían restablecer
contraseñas de otros
usuarios

GRAVEDAD: ALTA
PUNTUACIÓN: 9.8



CVE-2023-
21367

Debido a un mal diseño en
Scudo, atacantes podían
divulgar información sin la
necesidad de privilegios
de ejecución

GRAVEDAD: MEDIA
PUNTUACIÓN: 5.5

Contramedidas

- Incorporar medidas de seguridad en todas las fases del desarrollo de software.
- Establecer y utilizar un catálogo de patrones de diseño seguros
- Analizar los posibles ataques y vulnerabilidades en procesos clave
- Implementar controles y validaciones de seguridad en todas las capas del sistema

- Realizar pruebas para la comprobación de la resistencia a vulnerabilidades
- Separar las capas de sistema y red
- Realizar un aislamiento de los tenants (usuarios o clientes) en todos los niveles del sistema
- Limitar el consumo de recursos por usuario o servicio.



Software and Data Integrity Failures

Descripción

Este tipo de fallos sucede cuando la infraestructura no está correctamente protegido contra modificaciones sin autorización.

Estas pueden provenir de aplicaciones que dependan de repositorios, plugins, bibliotecas...



CVE



**CVE-2022-
31609**

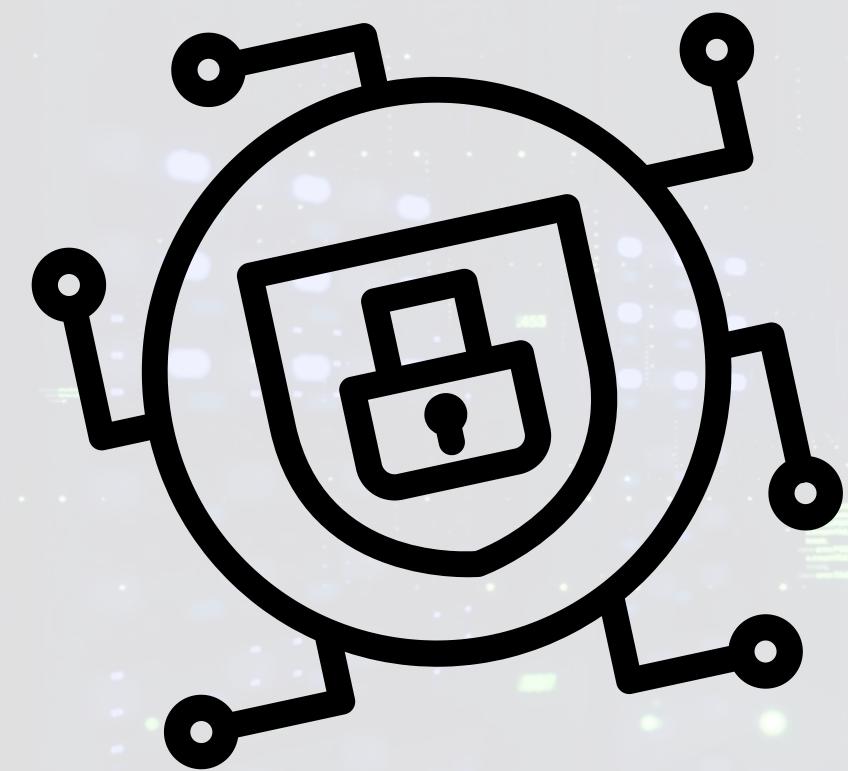
Vulnerabilidad en el software de NVIDIA vGPU, la cual permitía a máquinas invitadas asignarse recursos de los cuales no tenían autorización

GRAVEDAD: ALTA
PUNTUACIÓN: 7.8

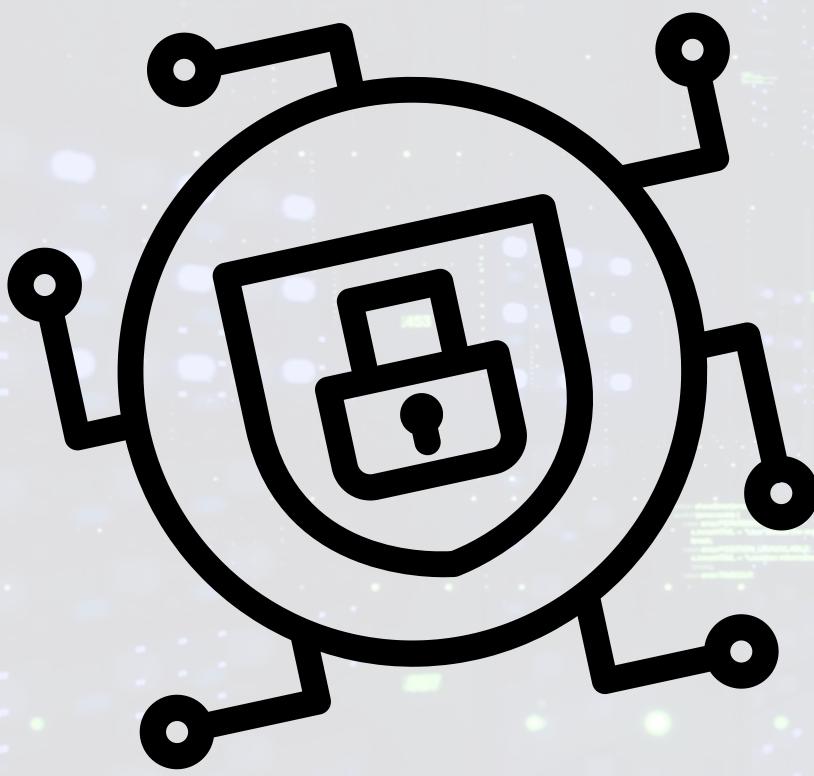
CONTRAMEDIDAS

- Verificación del origen de los software o datos.
- Utilizar repositorios confiables
- Verifica la ausencia de vulnerabilidades conocidas con el uso de herramientas
- Revisión de cambios en el código y las configuraciones
- Asegúrese que su pipeline CI/CD posee adecuados controles de acceso
- Asegúrate de no enviar datos sin proteger (sin cifrado o firma) a clientes no confiables





Conclusión



**Gracias por
su atención**

GRUPO 3