INFOVORE: I

INFORME EJECUTIVO

AUTOR

Guido Bruno Romano De Nardo

2025-04-08

Índice

1. Introducción

Este informe detalla una vulnerabilidad identificada en la máquina de prueba **Infovore 1 de la plataforma Vulnhub** (Ver en Vulnhub). La explotación de esta falla podría comprometer la seguridad del sistema y permitir accesos no autorizados. En este análisis, se examina el nivel de riesgo y se presentan estrategias de mitigación.

2. Descripción de la Vulnerabilidad

El servidor tiene el puerto 80 abierto, lo que normalmente permite que ciertos archivos y servicios sean accesibles desde internet. Durante la evaluación, **se identificó un archivo PHP que revela información técnica** sobre la configuración del servidor.

Este archivo está **configurado de tal manera que permite la carga de otros archivos en el servidor**, lo que puede facilitar ataques mediante una técnica conocida como Local File Inclusion (LFI). **Si un atacante explota esta vulnerabilidad, podría ejecutar comandos remotamente y tomar el control del servidor**.

3. Impacto Potencial

Si un atacante usa LFI con éxito, **podrá ingresar inicialmente a un contenedor**, que es un espacio aislado dentro del servidor. Aunque este contenedor no da acceso completo al sistema, **aquí se ha abierto el puerto 22, el cual permite conexiones remotas**, y está accesible desde este entorno.

Durante el análisis de este contenedor, **se encontró un archivo oculto llamado oldkeys.tgz**, que contiene una clave privada y una clave pública. Si un atacante logra descifrar la clave privada mediante herramientas automatizadas, podría obtener acceso privilegiado dentro del contenedor.

Desde ese punto, **el atacante podría escalar privilegios hasta obtener acceso de administrador y salir del contenedor para comprometer la máquina principal. Una vez dentro, podría aprovechar configuraciones del grupo Docker para incrementar aún más sus permisos, obteniendo control total sobre los archivos y otros contenedores en el servidor**.

4. Riesgos Asociados

- **Exposición de información sensible**: El archivo PHP revela detalles internos del servidor, facilitando futuros ataques.
- **Escalamiento de privilegios**: Un atacante podría obtener permisos administrativos sin autorización.
- **Acceso no autorizado**: Con privilegios elevados, el atacante puede ejecutar comandos maliciosos o modificar configuraciones críticas.
- **Compromiso de información**: Si el atacante logra el control del servidor, puede acceder y robar datos sensibles.

5. Recomendaciones y Medidas de Mitigación

- **Restringir el acceso al puerto 80**: Configurar reglas de firewall para limitar el acceso desde internet.
- **Eliminar o proteger el archivo PHP-info**: Revisar que la configuración del servidor no sea accesible públicamente.
- **Monitorear el tráfico del servidor**: Activar alertas que detecten accesos sospechosos o intentos de ataque.
- **Revisar permisos y configuraciones en Docker**: Restringir privilegios innecesarios para prevenir accesos no autorizados.
- **Fortalecer claves y credenciales**: No almacenar claves privadas en archivos visibles y utilizar métodos de cifrado robustos.

Cuadro 1: Resumen de vulnerabilidad y mitigaciones

Riesgo	Impacto	Solución
Exposición de información	Acceso no autorizado	Eliminación de archivos expuestos
Escalamiento de privilegios	Control total del servidor	Revisión de permisos
Compromiso de datos	Robo de información empresarial	Implementación de cifrado

6. Conclusión

La configuración del servidor Infovore 1 presenta un riesgo significativo porque permite que un atacante acceda a un contenedor y aumente sus privilegios hasta tomar el control de la máquina principal. La exposición de información interna y la reutilización de credenciales facilitan este proceso.

Las soluciones propuestas en este informe no solo corrigen la vulnerabilidad detectada, sino que también ayudan a reforzar la seguridad del sistema en general. Es fundamental limitar el acceso a servicios innecesarios, proteger archivos sensibles y mejorar la gestión de permisos para evitar accesos no autorizados.

Implementar estas medidas reducirá el riesgo de ataque y garantizará un entorno más seguro contra futuras amenazas.

La Tabla 1 resume los riesgos detectados y sus posibles soluciones.

Nomenclatura

Archivo oldkeys.tgz Archivo con claves de acceso.

Archivo PHP-info Archivo que muestra detalles técnicos del servidor.

Contenedor Entorno aislado dentro del servidor que ejecuta aplicaciones de forma independiente.

Credenciales privilegiadas Usuarios con permisos elevados en el sistema.

Escalamiento de privilegios Proceso mediante el cual un atacante obtiene mayores permisos.

Firewall Sistema de seguridad que bloquea o permite conexiones para proteger el servidor.

Grupo Docker Grupo de usuarios con acceso para administrar contenedores.

LFI (Local File Inclusion) Técnica usada para acceder y ejecutar archivos dentro del servidor.

Puerto 22 Canal usado para conexiones remotas seguras (SSH).

Puerto 80 Canal por donde viaja el tráfico web.

Reverse Shell Conexión remota que permite a un atacante controlar el sistema de manera encubierta.