Vulnerabilidades Detectadas en Servicios

Introducción
Este informe detalla las vulnerabilidades asociadas a los servicios Apache httpd y MariaDB detectados en el objetivo con IP 192.168.1.141. Se realizó una búsqueda en bases de datos públicas para identificar posibles vulnerabilidades que puedan comprometer el sistema.

Servicios Detectados

Apache httpd 2.4.62 (Debian):

- **Puerto:** 80/tcp
- **Descripción:** Apache HTTP Server es una de las plataformas de servidor web más comunes. La versión 2.4.62 en Debian puede ser vulnerable a varios tipos de ataques si no está correctamente configurada o actualizada.

MariaDB:

- **Puerto:** 3306/tcp
- **Descripción:** MariaDB es un sistema de gestión de bases de datos relacional. El acceso no autorizado sugiere que no se requiere autenticación para conectarse al servicio.

Vulnerabilidades Encontradas

Apache httpd 2.4.62 (Debian):

- **CVE-2024-38476:** Un problema en el manejo de redirecciones internas podría permitir ejecución de scripts locales maliciosos, provocando fuga de información o SSRF en ciertas aplicaciones.
- **CVE-2024-38477:** Un error en `mod_proxy` podría provocar una Denial of Service (DoS) si un atacante envía solicitudes maliciosas.
- **CVE-2024-39573:** Potencial SSRF a través de reglas de redirección en `mod_rewrite`.

MariaDB:

- **CVE-2022-24050:** Esta vulnerabilidad se relaciona con un problema de ***Use-After-Free*** que puede permitir a un atacante local ejecutar código arbitrario o provocar una denegación de servicio. Ocurre cuando el software intenta utilizar memoria que ha sido liberada. Afecta a todas las versiones anteriores a 10.2.42 y 10.3.33. Tiene un alto impacto. La vulnerabilidad puede comprometer la integridad, confidencialidad y disponibilidad del sistema. Se recomienda actualizar a una versión no vulnerable de MariaDB para mitigar el riesgo.

Impacto
Describir cómo estas vulnerabilidades podrían ser explotadas por un atacante y el impacto en el sistema, como acceso no autorizado, compromiso de datos, etc

Recomendaciones

- Actualizar Apache y MariaDB a las últimas versiones disponibles.
- Implementar reglas de firewall para restringir el acceso a servicios críticos.
- Configurar autenticación adecuada en MariaDB.

Conclusión
Las vulnerabilidades identificadas presentan riesgos significativos si no se abordan adecuadamente. Se recomienda realizar las actualizaciones necesarias y aplicar las configuraciones de seguridad recomendadas para mitigar los posibles ataques.