A05-2021 Security Misconfiguration

Son los errores o configuraciones inapropiadas en el entorno, la aplicación o los servicios utilizados, que exponen el sistema a riesgos innecesarios, esta falla puede incluir en:

- Configuraciones por defectos no seguras.
- Exposiciones innecesaria de información.
- Permisos excesivos en archivo o servicios.

Ejemplo: Almacenamiento en la nube con permisos públicos, o instancias de bases de datos expuestas a internet.

Gravedad

- Impacta en múltiples niveles: Desde la aplicación hasta la infraestructura subyacente.
- Facilidad de explotación: A menudo, los atacantes solo necesitan explorar configuraciones públicas o aprovechar configuraciones por defecto.
- Amplitud del impacto: Puede facilitar otros ataques como escalada de privilegios, inyección de código o acceso no autorizado.

Mitigación

- Endurecimiento del servidor: Aplicar configuraciones de seguridad recomendadas para el sistema operativo, el servidor web y la base de datos.
- Seguridad en la nube: Revisar y endurecer las configuraciones de seguridad de los servicios en la nube utilizados.
- Gestión de secretos: Almacenar las credenciales y otros secretos de forma segura, evitando incluirlos en el código fuente.
- Análisis de seguridad de la configuración: Usar herramientas para escanear y detectar configuraciones inseguras.
- Política de seguridad de la información: Es importante que las empresas tengan políticas de seguridad de la información, que ayuden a los empleados a la correcta configuración de los sistemas.