A09-2021 Security Logging and Monitoring Failures

Es la falta de registros adecuados o la incapacidad de monitorear eventos críticos relacionados con la seguridad, lo que dificulta la detección, el análisis y la respuesta a incidentes de seguridad. Esto puede incluir:

- Falta de registros de actividad clave.
- Registros insuficientes, incorrectos o inaccesibles durante un incidente.
- Monitorea ineficaz o ausente de eventos críticos.

Ejemplos: Una aplicación que no registra intentos fallidos de inicio de sesión, dificultando la identificación de un ataque de fuerza bruta.

Gravedad

- **Facilita ataques prolongados**: La falta de monitoreo permite a los atacantes operar sin ser detectados durante largos períodos.
- **Dificulta la respuesta a incidentes**: Sin registros adecuados, es casi imposible determinar cómo ocurrió un ataque o qué datos fueron comprometidos.
- **Impacto en la reputación y cumplimiento**: Muchas regulaciones (como GDPR o PCI DSS) exigen el registro y monitoreo de eventos; su ausencia puede llevar a sanciones legales.

Mitigación

- **Análisis de registros**: Utilizar herramientas de análisis de registros para identificar patrones y anomalías en los registros de seguridad.
- **Inteligencia de amenazas**: Integrar información de inteligencia de amenazas en los sistemas de monitoreo para detectar actividades maliciosas conocidas.
- **Respuesta a incidentes**: Desarrollar un plan de respuesta a incidentes claro y conciso que incluya procedimientos para la investigación y la contención de incidentes de seguridad.
- **Política de registro y monitoreo**: Es muy importante que las empresas tengan politicas de registro y monitoreo, para que los encargados de los sistemas puedan tener un correcto manejo de este tipo de problemas.