A08-2021 Software and Data Integrity Failures

Es la incapacidad de garantizar que el software y los datos no han sido manipulados o alterados de manera maliciosa durante su desarrollo, distribución o ejecución. Esto puede incluir:

- Uso de actualizaciones de software o librerías sin verificar su integridad.
- Falta de validación de firmas digitales en paquetes o datos.
- Dependencia de fuentes no confiables para la adquisición de software o componentes.

Ejemplo: Atacantes que comprometen repositorios de software o herramientas de desarrollo para inyectar código malicioso.

Gravedad

- Impacto severo: Permite a atacantes inyectar código malicioso en software o manipular datos sensibles.
- Riesgo extendido: Las fallas de integridad pueden propagarse a múltiples usuarios o sistemas afectados.
- Casos difíciles de detectar: La manipulación de software o datos puede permanecer oculta durante largos períodos.

Mitigación

- Firmas de código: Implementar la firma de código para verificar la autenticidad y la integridad del software.
- Listas de materiales de software (SBOM): Generar y mantener SBOM para rastrear las dependencias de software.
- Entornos de ejecución seguros: Utilizar entornos de ejecución seguros que restrinjan el acceso a recursos críticos.
- Política de gestión de la cadena de suministro: Es necesario que las empresas tengan politicas de gestión de la cadena de suministro, para que los encargados de los sistemas puedan tener un correcto manejo de este tipo de problemas.