A06-2021 Vulnerable and Outdated Components

Es el uso de bibliotecas, frameworks, módulos, sistemas operativos, servidores web y cualquier otro software utilizado en el sistema, que posea vulnerabilidades conocidas o que están desactualizados. Esto ocurre cuando:

- Se utilizan versiones antiguas con problemas de seguridad ya reportados.
- No se aplican parches o actualizaciones críticas.
- Se integran dependencias sin verificar su seguridad.

Ejemplo: Servidores que ejecutan versiones antiguas de Linux o Windows sin parches de seguridad.

Gravedad

- Amplia explotación: Los atacantes suelen buscar versiones específicas con vulnerabilidades conocidas y herramientas automatizadas para explotarlas.
- Impacto sistémico: Puede comprometer no solo una aplicación, sino todo el ecosistema si el componente es ampliamente utilizado.
- Difícil de mitigar en sistemas complejos: En proyectos con muchas dependencias, identificar y actualizar todos los componentes puede ser complicado.

Mitigación

- Automatización de actualizaciones: Implementar herramientas de automatización para mantener actualizados los componentes y las dependencias.
- Análisis de composición de software (SCA): Utilizar herramientas de SCA para identificar y gestionar las dependencias de software.
- Listas de vulnerabilidades conocidas (CVE): Mantenerse informado sobre las vulnerabilidades conocidas a través de fuentes como la base de datos CVE.
- Política de gestión de vulnerabilidades: Es necesario que las empresas tengan politicas de gestión de vulnerabilidades, para que los encargados de los sistemas puedan tener un correcto manejo de este tipo de problemas.