A10-2021 Server-Side Request Forgery (SSRF)

Ocurre cuando una aplicación web permite que un atacante manipule y envié solicitudes a servidores internos o externos en nombres del servidor vulnerable. Esto sucede típicamente debido a una validación insuficiente de las entradas proporcionadas por el usuario, lo que permite al atacante:

- Acceder a recursos internos de la red.
- Ejecutar ataques adicionales, como extracción de datos o escaneo de puertos internos.
- Realizar solicitudes maliciosas hacia servidores externos.

Ejemplo: Un atacante podría utilizar SSRF para acceder a bases de datos internas, servidores de administración o APIs internas.

Gravedad

- Amplitud del impacto: Puede usarse para acceder a redes internas, potencialmente exponiendo información sensible o servicios internos no protegidos.
- Facilidad de explotación: Muchas aplicaciones confían en las entradas del usuario para generar solicitudes sin validación adecuada.
- Base para ataques secundarios: Puede habilitar ataques como la ejecución remota de código, extracción de metadatos en la nube o el compromiso de sistemas internos.

Mitigación

- Listas blancas de URLs: Permitir solo solicitudes a URLs o dominios específicos.
- Deshabilitar redirecciones: Evitar el uso de funciones que permitan redirecciones sin validación.
- Aislamiento de redes: Aislar los servidores internos de la red externa para limitar el impacto de un ataque SSRF.
- Política de seguridad de peticiones: Es muy importante que las empresas tengan políticas de seguridad de peticiones, para que los encargados de los sistemas puedan tener un correcto manejo de este tipo de problemas.