A07-2021 Identification and Authentication Failures

Abarca una amplia gama de errores en la gestión de identidades y la autenticación de usuarios. Es crucial entender que la autenticación no solo verifica la identidad del usuario, sino que también establece la base para la autorización. Esto se puede dar por:

- Uso de contraseñas débiles o predeterminadas.
- Falta de protección contra ataques de fuerza bruta.
- Implementación incorrecta de funciones como el restablecimiento de contraseñas o el manejo de tokens de sesión.

Ejemplo: No validar adecuadamente los códigos de MFA o permitir eludir la MFA.

Gravedad

- **Impacto directo en la seguridad del sistema**: Permite a los atacantes acceder a cuentas y datos sensibles.
- **Riesgo de escalada de privilegios**: Una cuenta comprometida puede usarse para obtener acceso adicional en el sistema.
- **Facilidad de explotación**: Las fallas en autenticación son frecuentemente explotadas con herramientas automatizadas para fuerza bruta o recolección de credenciales.

Mitigación

- **Implementación de la autenticación adaptativa**: Utilizar información contextual, como la ubicación o el dispositivo del usuario, para evaluar el riesgo de inicio de sesión.
- **Gestión de identidades y accesos (IAM)**: Implementar soluciones de IAM para gestionar las identidades y los accesos de los usuarios de forma centralizada.
- **Pruebas de seguridad de la autenticación**: Realizar pruebas de seguridad específicas para la autenticación, como pruebas de fuerza bruta, pruebas de relleno de credenciales y pruebas de bypass de MFA.
- **Política de contraseñas robusta**: Es necesario que las empresas tengan políticas de contraseñas robustas, que ayuden a los usuarios a generar contraseñas seguras y a tener un correcto manejo de ellas.