A07-2021 Identification and Authentication Failures

It covers a wide range of errors in identity management and user authentication. It is crucial to understand that authentication not only verifies the user's identity, but also establishes the basis for authorization. This can occur due to:

- Use of weak or default passwords.
- Lack of protection against brute-force attacks.
- Incorrect implementation of functions such as password reset or session token handling.

Example: Not properly validating MFA codes or allowing MFA bypass.

Severity

- Direct impact on system security: Allows attackers to access accounts and sensitive data.
- Risk of privilege escalation: A compromised account can be used to gain additional access to the system.
- Ease of exploitation: Authentication failures are frequently exploited with automated tools for brute-force or credential harvesting.

Mitigation

- Adaptive authentication implementation: Use contextual information, such as user location or device, to assess login risk.
- Identity and Access Management (IAM): Implement IAM solutions to centrally manage user identities and access.
- Authentication security testing: Perform specific security tests for authentication, such as brute-force tests, credential stuffing tests, and MFA bypass tests.
- Robust password policy: It is necessary for companies to have robust password policies, which help users generate secure passwords and have correct handling of them.