A02-2021 Cryptographic Failures

It refers to problems related to the incorrect implementation or absence of cryptographic measures necessary to protect sensitive data. Failures may include:

- Use of weak or obsolete cryptographic algorithms.
- Transmission of sensitive data without encryption.
- Insecure storage of cryptographic keys.
  Example: Storing passwords in plain text or transmitting confidential information without encryption.

Severity

The risk is high especially in systems that handle sensitive, financial or authentication data.

- Exposure of sensitive data: Allows cybercriminals to access, modify or steal confidential information.
- Breach of confidentiality and integrity: Can compromise user trust and security.
- Impact on regulatory compliance: Violations of GDPR, HIPPA or other data protection regulations.

Mitigation

1. Data encryption in transit and at rest:

- Use secure protocols such as TLS 1.2 or higher for transmission.
- Ensure that sensitive data stored is encrypted with modern algorithms such as AES-256.

2. Avoid insecure algorithms:

- Do not use obsolete algorithms such as MD5 or SHA-1.
- Use updated standards such as SHA-256 or higher

3. Proper management of cryptographic keys:

- Store keys in secure modules and not in source code or exposed locations.

4. Validate security configurations:

- Correctly configure cryptographic protocols and tools, avoiding weak or default configurations.