A04-2021 Insecure Design

It focuses on deficiencies at the architectural and design level, that is, before code implementation. This implies that security must be a primary consideration from the beginning of the software development life cycle. Unlike other categories that focus on specific implementation errors, insecure design is a systemic problem that can lead to multiple vulnerabilities.

Example: Not separating internal and external networks, which allows an attack on one network to affect others.

Severity

- Causes structural problems: Design flaws affect the entire system and are often difficult to correct without significant restructuring.
- Enables other vulnerabilities: An insecure design can facilitate the exploitation of problems such as injection, weak access control, etc.
- Long-term risk: Poorly designed systems are more likely to fail against future threats.

Mitigation

- Threat modeling: Perform threat analysis to identify potential attack vectors and design security controls to mitigate them.
- Secure reference architecture: Use secure reference architectures and proven design patterns.
- Security design reviews: Perform regular security design reviews to identify and correct potential vulnerabilities.
- Risk-based development: Prioritize security activities based on the risk posed by different functionalities and system components.