A05-2021 Security Misconfiguration

They are errors or inappropriate configurations in the environment, application, or services used, which expose the system to unnecessary risks. This flaw can include:

- Insecure default configurations.
- Unnecessary exposure of information.
- Excessive permissions on files or services.

Example: Cloud storage with public permissions, or database instances exposed to the internet.

Severity

- Impacts multiple levels: From the application to the underlying infrastructure.
- Ease of exploitation: Often, attackers only need to explore public configurations or take advantage of default settings.
- Scope of impact: It can facilitate other attacks such as privilege escalation, code injection, or unauthorized access.

Mitigation

- Server hardening: Apply recommended security configurations for the operating system, web server, and database.
- Cloud security: Review and harden the security configurations of the cloud services used.
- Secrets management: Store credentials and other secrets securely, avoiding including them in the source code.
- Configuration security analysis: Use tools to scan and detect insecure configurations.
- Information security policy: It is important that companies have information security policies that help employees correctly configure systems.