A08-2021 Software and Data Integrity Failures

It is the inability to ensure that software and data have not been maliciously manipulated or altered during their development, distribution, or execution. This can include:

- Use of software or library updates without verifying their integrity.
- Lack of digital signature validation in packages or data.
- Dependence on untrusted sources for software or component acquisition.

Example: Attackers who compromise software repositories or development tools to inject malicious code.

Severity

- Severe impact: Allows attackers to inject malicious code into software or manipulate sensitive data.
- Extended risk: Integrity failures can spread to multiple affected users or systems.
- Difficult to detect cases: Software or data manipulation can remain hidden for long periods.

Mitigation

- Code signing: Implement code signing to verify the authenticity and integrity of the software.
- Software Bill of Materials (SBOM): Generate and maintain SBOMs to track software dependencies.
- Secure execution environments: Use secure execution environments that restrict access to critical resources.
- Supply chain management policy: It is necessary for companies to have supply chain management policies, so that those responsible for the systems can have a correct handling of this type of problem.