A06-2021 Vulnerable and Outdated Components

It is the use of libraries, frameworks, modules, operating systems, web servers, and any other software used in the system, that have known vulnerabilities or are outdated. This occurs when:

- Old versions with already reported security problems are used.
- Critical patches or updates are not applied.
- Dependencies are integrated without verifying their security.

Example: Servers running old versions of Linux or Windows without security patches.

Severity

- Wide exploitation: Attackers often look for specific versions with known vulnerabilities and automated tools to exploit them.
- Systemic impact: It can compromise not only an application, but the entire ecosystem if the component is widely used.
- Difficult to mitigate in complex systems: In projects with many dependencies, identifying and updating all components can be complicated.

Mitigation

- Update automation: Implement automation tools to keep components and dependencies up to date.
- Software Composition Analysis (SCA): Use SCA tools to identify and manage software dependencies.
- Common Vulnerabilities and Exposures (CVE) lists: Stay informed about known vulnerabilities through sources such as the CVE database.
- Vulnerability management policy: It is necessary for companies to have vulnerability management policies, so that those responsible for the systems can have a correct handling of this type of problem.