Dependency Confusion

> A dependency confusion attack or supply chain substitution attack occurs when a software installer script is tricked into pulling a malicious code file from a public repository instead of the intended file of the same name from an internal repository.

Summary

Tools

- Confused

Exploit

Look for `npm`, `pip`, `gem` packages, the methodology is the same : you register a public package with the same name of private one used by the company and then you wait for it to be used.

NPM example

- List all the packages (ie: package.json, composer.json, ...)
- Find the package missing from https://www.npmjs.com/
- Register and create a **public** package with the same name
    - Package example : https://github.com/0xsapra/dependency-confusion-expoit

References

- Exploiting Dependency Confusion - 2 Jul 2021 - 0xsapra
- Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies - Alex Birsan - 9 Feb 2021
- Ways to Mitigate Risk When Using Private Package Feeds - Microsoft - 29/03/2021
- $130,000+ Learn New Hacking Technique in 2021 - Dependency Confusion - Bug Bounty Reports Explained