Attacking the Supply Chain

Abhinav Vasisth &
Nishaanth Guna

Table of contents

Introduction

$ whoami

Abhinav Vasisth, Senior Security Researcher @Appknox
Nishaanth Guna, Senior Security Researcher @Appknox

Primarily work on Android and iOS Security Assessments and Research.
Hall of fames and 0-days in Apple, Microsoft, AT&T, Govt. of UK among others.

What is a supply chain? System designed to supply products and services

Components of the Supply chain in development

1. Code
2. Package Managers
3. Binaries from other resources
4. Repositories
5. Anything else needed to delivery your product or service

Current Problems

Package Managers

- Inability to monitor malicious packages
- Difficulty in changing owners
- Large amount of trust placed on very few package managers Eg: npm, pip
- Large amount of burden placed on Producers and consumers

Client Side Installation

- Not knowing the status of a package (deprecated, unmaintained, broken, missing etc)
- Package and Import names are different

Attack Methods to Exploit

Package and Import names Mismatch

Multiple Indexes in CLI : --extra-index-url

Deleted Sources : Prone to Hijacking

DEMO

What can you do?

- For pip,use index-url by default
- Protect packages from being hijacked using controlled scopes.
- Specify precise versions for packages and dependencies to mitigate forced upgrade or downgrade attacks.

Thanks!

References

- https://azure.microsoft.com/mediahandler/files/resourcefiles/3-ways-to-mitigate-risk-using-private-package-feeds/3%20Ways%20to%20Mitigate%20Risk%20When%20Using%20Private%20Package%20Feeds%20-%20v1.0.pdf
- https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610
- https://github.com/ipfs-inactive/package-managers/issues/17
- https://redhuntlabs.com/blog/dependency-confusion-attack-what-why-and-how.html
- https://github.blog/2020-09-02-secure-your-software-supply-chain-and-protect-against-supply-chain-threats-github-blog/