The Common Pitfalls of Cloud Native Software Supply Chains

Daniel Shapira @Palo Alto Networks
Source Code

Version Control & Build tools

Developers
Version Control & build tools
Version Control & build tools

- Subversion
- Mercurial
- Visual Studio Team Foundation Server
- CVS
Version Control & build tools

Mature & considered safe
Version Control & build tools

Mature & considered safe

*As long as they are authentic*
Fake tool-chains
Fake tool-chains

XcodeGhost - a malicious Xcode version
Fake tool-chains

XcodeGhost - a malicious Xcode version

WeChat compiled with it and it infected 600,000,000 end-users
Fake tool-chains

XcodeGhost - a malicious Xcode version

WeChat compiled with it and it infected 600,000,000 end-users
Verify authenticity & integrity
Verify authenticity & integrity

• Create a single source of truth for your tools
Verify authenticity & integrity

- Create a single source of truth for your tools
- Verify by matching hash sums
Verify authenticity & integrity

- Create a single source of truth for your tools
- Verify by matching hash sums
- Make sure your source of truth is secure
• Fuzzing - providing invalid, unexpected, or random inputs, and monitoring for misbehavior
Fuzzing

- Fuzzing - providing invalid, unexpected, or random inputs, and monitoring for misbehavior
- Continuous fuzzing is constantly having a fuzz test running, only restarting when new code is introduced
Fuzzing

- Fuzzing - providing invalid, unexpected, or random inputs, and monitoring for misbehavior
- Continuous fuzzing is constantly having a fuzz test running, only restarting when new code is introduced

Tools:
- go-fuzz
- libFuzzer
- american fuzzy lop
- clusterfuzz
Commit

Private repository

Public repository
Commit

Private repository

Public repository
Commit

Private repository

Public repository
Secrets in public repos

• Once you have pushed a commit, you should consider any data it contains to be compromised
Secrets in public repos

- Once you have pushed a commit, you should consider any data it contains to be compromised
- If you committed a password, change it!
- If you committed a key, generate a new one
Secrets in public repos

- Once you have pushed a commit, you should consider any data it contains to be compromised
- If you committed a password, change it!
- If you committed a key, generate a new one
- Monitor and prevent future commits containing secrets
Secrets in public repos

- Once you have pushed a commit, you should consider any data it contains to be compromised
- If you committed a password, change it!
- If you committed a key, generate a new one
- Monitor and prevent future commits containing secrets

Tools for the job:
- Git-Hound, Git-secrets,
- TruffleHog, Gitrob, etc...
The Common Pitfalls of Cloud Native Software Supply Chains

Daniel Shapira @Palo Alto Networks

- Source Code
- CI/CD
- Universal package managers
- Publishing infrastructure
- Q & A
CVEs
CVEs

- CVE - a list of entries for publicly known vulnerabilities
CVEs

- CVE - a list of entries for publicly known vulnerabilities
- Over 300 CVEs in old versions of CI/CD tools
CVEs

- CVE - a list of entries for publicly known vulnerabilities
- Over 300 CVEs in old versions of CI/CD tools
- 60% of which were reported during 2019 alone
CVEs

• CVE - a list of entries for publicly known vulnerabilities

• Over 300 CVEs in old versions of CI/CD tools

• 60% of which were reported during 2019 alone

• A CVE is your mark to upgrade!
Secrets

- If secrets are not leaking from version control, they might leak from your CI
Secrets

- If secrets are not leaking from version control, they might leak from your CI
- Build history may contain sensitive information
Secrets

• If secrets are not leaking from version control, they might leak from your CI

• Build history may contain sensitive information

• Anyone who can create jobs on Jenkins can uncover all Global secrets
Misconfigurations
Misconfigurations

- Anonymous access allowed
Misconfigurations

- Anonymous access allowed
- Instances publicly exposed
Misconfigurations

- Anonymous access allowed
- Instances publicly exposed
- Over-permissive privileges given
Misconfigurations

- Anonymous access allowed
- Instances publicly exposed
- Over-permissive privileges given
- Authentication is not enforced everywhere
The Common Pitfalls of Cloud Native Software Supply Chains

Daniel Shapira @Palo Alto Networks
Universal Package Managers

- Archiva
- CloudRepo
- Cloudsmith
- ProGet
- JFrog Artifactory

Auth & Authz
Authentication & Authorization
Authentication & Authorization

• Authentication is the Achilles heel
Authentication & Authorization

- Authentication is the Achilles heel
- Dangerously over-permissive default settings
The Common Pitfalls of Cloud Native Software Supply Chains

Daniel Shapira @Palo Alto Networks
Containers
Containers

- Restricted processes chrooted to a separate filesystem
Containers
Containers

- docker run
Containers
Containers

Docker run → runc init → execve /bin/sleep → /bin/sleep
Containers

- `docker run ubuntu sleep`
Containers

/bin/sleep

Container
Containers

- docker run ubuntu sleep
Containers - attack surface

• Container escape

How?

1. malicious container images
2. breached container
Containers - Copy command
Containers - Copy command

- Copy from a container to host
- Copy from host to container
- Copy between containers

> docker cp /tmp/file ubuntu_container:/tmp/file

> podman cp host_file ubuntu_container:/dir/abc
Copy command - Podman

> podman cp host_file ubuntu_container:/dir/abc

- Build container path (from host’s view)
  - /var/lib/.../$container_id/merged + /dir/abc

- Then preform copy
  - cp host_file /var/lib/.../$container_id/merged/dir/abc
Podman - the problem

- Symlinks!

- Symlink - a file that contains a reference to another file or directory
Podman - CVE-2019-10152

- Symlinks resolved under host root

- symlink "fake_directory=>/critical/path"

```bash
> podman cp host_file container:/fake_directory/file
```

result: /critical/path/file
Copy command - Docker

- 1. Resolve container path in container root
- 2. Add resolved path to container mount point
- 3. Perform copy operation
Copy command - Docker

fake_directory => /critical/path

> docker cp host_file container:/fake_directory/file

1. /critical/path/file

2. /var/lib/..../$container_id/merged + /critical/path/file

3. cp host_file /var/lib/..../$container_id/merged/critical/path/file
Docker CVE-2018-15664

- Symlink exchange race attack

> docker cp /host_file container:/somedir/file

1. /somedir/file
2. /var/lib/..../$container_id/merged + /somedir/file
   `somedir => /critical/path`
3. cp /host_file /var/lib/.../merged/somedir/file
   `/critical/path/file`
The Common Pitfalls of Cloud Native Software Supply Chains

Daniel Shapira @Palo Alto Networks
Questions?

Thank you!
Thank you!

Contact Me:
dshapira@paloaltonetworks.com
@Da5h_Solo

references:
https://cutt.ly/Open-Registries
https://cutt.ly/Escaping-Docker
more to be published soon :)

graphics from:
https://www.freepik.com
The Common Pitfalls of Cloud Native Software Supply Chains

Daniel Shapira @Palo Alto Networks