Containerskanning

Sårbarheter i en container

- Problem i egen kod
- Tredjepartsprogram

Vad är en containerskanner?

- Identifierar mjukvara som finns i containern
- Matchar mjukvaran mot en sårbarhetsdatabas
- Exempel:
  - Grype
  - Trivy

Demo: containerskanner

Hur hittas CVEs?

- OS-identifiering
- Pakethanterare
- Metadata från binärer

Demo: beroende av pakethantering

- Viktigt att containerskannern kan identifiera OS
- Manipulering av pakethanteringsdatabasen kan lura skannern

Flerstegsbyggen

- Vanligt sätt för att paketera mjukvara
- Kompilera i en container, för över till en annan

Demo: flerstegsbygge

Software Bill of Materials

- Lista på den mjukvara som ingår i en container

Demo: SBOM

Sammanfattning

- Skanners hittar CVEs i containrar
- Deras funktion kan saboteras
- Flerstegsbyggen är bra, men kräver att man anpassar skanningen
- 0 CVEs vid skanning garanterar ej CVE-fri container
- SBOM-generering påverkas också

https://youtu.be/9weGi0csBZM