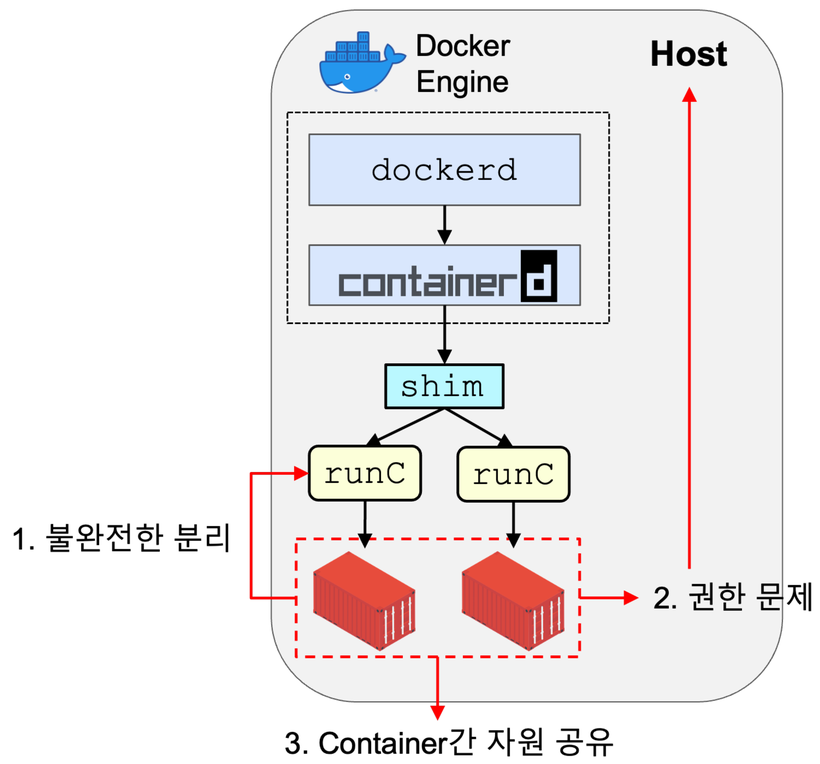
도커 컨테이너 취약점 동향 분석

김동은†, 이준희†, 김진우 ‡*
광운대학교 (학부생†, 교수‡)
*Corresponding author

컨테이너 구조의 문제점



1. 불완전한 분리

- 가상머신과는 달리 동일한 커널을 공유한다는 특징 때문에 컨테이너에서 호스트로 커널을 타고 접근하는 Container Escape 공격 등이 이루어질 수 있다.

2. 권한 문제

- 도커 엔진이나 리눅스 커맨드에 권한에 관련된 문제가 존재하는 경우 이를 이용하여 호스트 권한으로 상승시키는 Privilege Escalation나 호스트 파일에 접근하는 Host File Access가 이루어질 수 있다.

3. 컨테이너 간 자원 공유

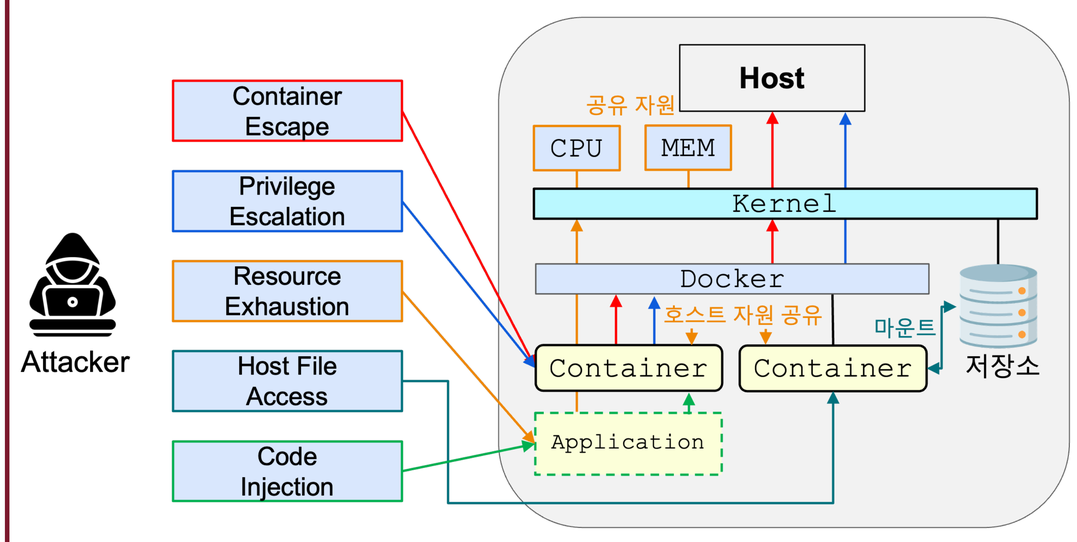
- 컨테이너는 호스트의 자원을 공유하여 사용하기에 특정 컨테이너에 Exhaustion 공격을 가해 다른 컨테이너에 영향을 주는 것이 가능하다.

취약점 동향 및 분류

Category	CVE	Summary	Image	Container Core
Container Escape	CVE-2022-39321	GitHub Action	O	O
	CVE-2022-0185	legacy_parse_param	O	X
	CVE-2019-5736	runC	X	O
Privilege Escalation	CVE-2022-24769	Moby process	X	O
	CVE-2022-36109	Moby group	X	O
	CVE-2018-15664	docker cp	X	O
Resource Exhaustion	CVE-2022-23471	containerd CRI	X	O
	CVE-2019-9073	BFD Library	O	X
	CVE-2021-39939	GitLab	O	X
Host File Access	CVE-2022-23648	containerd CRI	X	O
	CVE-2021-25741	Volume mount	X	O
	CVE-2019-11246	kubectl cp	X	O
Code Injection	CVE-2021-1560	Cisco DNA Space Connector	X	O
	CVE-2023-26490	mailcow	O	O
	CVE-2021-34079	Mintzo Docker-Tester	O	X

- 조사한 CVE 36개 중 74%가 컨테이너의 취약점을 이용한 공격이다.
- 최근에는 어플리케이션이 컨테이너의 취약점을 유발시키는 공격이 많다.
- 위 분류 포함, 본 연구에서 조사한 공개된 PoC 20개 중 10개는 악성 이미지를 이용한다.

취약점 위험도 분석



1. Container Escape

- 컨테이너의 고질적인 문제인 커널의 불완전한 격리를 이용하여 호스트에 접근하는 점에서 범용적이고 가장 위험도가 높은 공격이다.

2. Privilege Escalation

- 도커 엔진이나 리눅스 커맨드 등의 권한 취약점을 이용하여 호스트에 접근한다는 점에서 범용적이진 않지만 위험도가 높은 공격이다.

3. Resource Exhaustion

- 컨테이너들이 호스트의 자원을 공유한다는 것을 이용하여 특정 컨테이너를 공격하여 모든 컨테이너에 영향을 준다는 점에서 범용적이지만 호스트에 접근하는 위 두 공격에 비해 위험도는 낮다.

4. Host File Access

- 파일 시스템의 마운트나 권한 부여의 취약점을 이용한다는 점에서 범용성이 떨어지고 파일에만 접근한다는 점에서 위험도도 가장 낮다

5. Code Injection

- 프로토콜이나 어플리케이션의 입력에 대한 취약점을 이용한다는 점에서 컨테이너의 특성을 이용하지 못하기에 범용도를 측정하기 어렵고, 종류에 따라 위험도도 다르기에 측정하기 어렵다.

컨테이너 보안 가이드라인

1. 컨테이너 권한 최소화

- 컨테이너에 부여하는 권한(생성, 마운트)을 최소화 하면 권한에 관련된 취약점 Privilege Escalation, Host File Access, Container Escape를 보완할 수 있다.

2. 도커 및 이미지 최신화

- 최신화된 도커 엔진 및 이미지의 경우 발견된 취약점 전체에 대한 검토가 이루어지므로 본 논문에서 분류한 취약점 전부에 대해 안전하다.

3. 인증된 이미지 사용

- 분류된 취약점 중 명령어를 통한 공격을 제외하면 전부 악성 이미지를 통한 공격이 가능하고 특히 Container Core를 이용하는 Container Escape, Privilege Escalation은 악성 이미지로만 가능한 경우가 있다.
- 도커에서 인증하는 이미지를 사용할 경우, 이들 공격에 대한 예방이 가능하다.

Acknowledgement: 이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2022-00166401)