docker 진단결과 (페이지 1)

구분	진단코드	진단항목	취약도	점검결과
Host설정	DO-01	도커 최신 패치 적용	상	양호
Host설정	DO-02	도커 그룹에 불필요한 사용자 제거	중	양호
Host설정	DO-03	Docker daemon audit 설정	상	N/A
Host설정	DO-04	/var/lib/docker audit 설정	상	N/A
Host설정	DO-05	/etc/docker audit 설정	상	N/A
Host설정	DO-06	docker.service audit 설정	상	N/A
Host설정	DO-07	docker.socket audit 설정	상	N/A
Host설정	DO-08	/etc/default/docker audit 설정	상	N/A
도커 데몬 설정	DO-09	default bridge를 통한 컨테이너 간 네트워크 트래픽 제한	상	취약
도커 데몬 설정	DO-10	도커 클라이언트 인증 활성화	상	취약
도커 데몬 설정	DO-11	legacy registry (v1) 비활성화	하	취약
도커 데몬 설정	DO-12	추가 권한 획득으로부터 컨테이너 제한	상	N/A
도커 데몬 설정 파일	DO-13	docker.service 소유권 설정	상	양호
도커 데몬 설정 파일	DO-14	docker.service 파일 접근권한 설정	상	양호
도커 데몬 설정 파일	DO-15	docker.socket 소유권 설정	상	양호
도커 데몬 설정 파일	DO-16	docker.socket 파일 접근권한 설정	상	양호
도커 데몬 설정 파일	DO-17	/etc/docker 디렉터리 소유권 설정	상	양호
도커 데몬 설정 파일	DO-18	/etc/docker 디렉터리 접근권한 설정	상	양호
도커 데몬 설정 파일	DO-19	/var/run/docker.sock 파일 소유권 설정	상	양호
도커 데몬 설정 파일	DO-20	/var/run/docker.sock 접근권한 설정	상	N/A

docker 진단결과 (페이지 2)

구분	진단코드	진단항목	취약도	점검결과
도커 데몬 설정 파일	DO-21	daemon.json 파일 소유권 설정	상	N/A
도커 데몬 설정 파일	DO-22	daemon.json 파일 접근권한 설정	상	N/A
도커 데몬 설정 파일	DO-23	/etc/default.docker 파일 소유권 설정	상	양호
도커 데몬 설정 파일	DO-24	/etc/default.docker 파일 접근권한 설정	상	N/A
컨테이너 이미지 및 빌드 파일	DO-25	root가 아닌 user로 컨테이너 실행	중	양호
컨테이너 이미지 및 빌드 파일	DO-26	도커를 위한 컨텐츠 신뢰성 활성화	중	취약
컨테이너 런타임	DO-27	컨테이너 SELinux 보안 옵션 설정	중	N/A
컨테이너 런타임	DO-28	컨테이너에서 ssh 사용 금지	상	양호
컨테이너 런타임	DO-29	컨테이너에 privileged 포트 매핑 금지	중	양호
컨테이너 런타임	DO-30	PIDs cgroup 제한	상	양호
컨테이너 런타임	DO-31	도커의 default bridge docker0 사용 제한	하	취약
컨테이너 런타임	DO-32	호스트의 user namespaces 공유 제한	하	양호

docker 조치사항 (페이지1)

진단코드	진단항목	조치방법
DO-09	default bridge를 통한 컨테이너 간 네트워크 트래픽 제한	dockerd --icc=false로 데몬 재시작 /etc/default/docker 파일에 DOCKER_OPTS="--icc=false"옵션 추가 후 데몬 재시작 /etc/docker/daemon.json 파일에 { "icc": false } 추가 후 데몬 재시작
DO-10	도커 클라이언트 인증 활성화	docker daemon --authorization-plugin=<PLUGIN_ID> /etc/default/docker 파일에 DOCKER_OPTS=" --authorization-plugin<PLUGIN_ID>"추가 후 데몬 재시작 /etc/docker/daemon.json 파일에 아래와 같은 옵션 추가 후 데몬 재시작 { "authorization-plugins": ["PLUGIN_ID"]}
DO-11	legacy registry (v1) 비활성화	$ docker daemon--disable-legacy-registry 데몬 시작 후 /etc/default/docker 파일에 DOCKER_OPTS="--disable-legacy-registry" 옵션 추가 후 데몬 재시작
DO-26	도커를 위한 컨텐츠 신뢰성 활성화	$ export DOCKER_CONTENT_TRUST=1 사용하는 shell(예. bash shell)에 아래와 같은 내용을 추가
DO-31	도커의 default bridge docker0 사용 제한	사용자 정의 네트워크를 설정하고, 정의된 네트워크에서 컨테이너를 실행