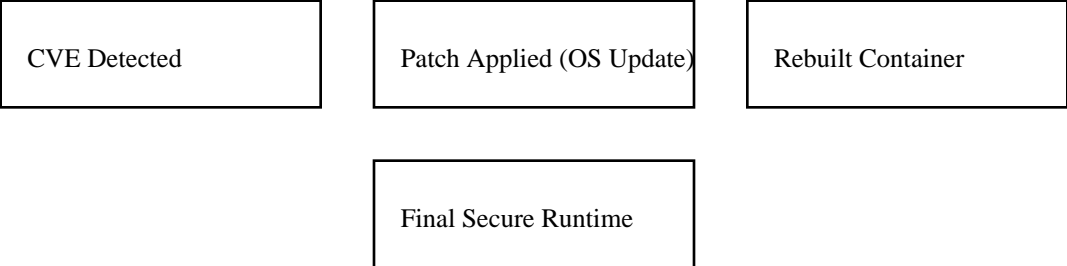


# How We Mitigate CVEs in Modern Container Images

Mitigating Common Vulnerabilities and Exposures (CVEs) in container images is critical for ensuring production-grade security. Modern applications often bundle OS-level packages, runtimes, and dependencies that may contain vulnerabilities. Effective mitigation involves updating the underlying base image, applying OS patches, and ensuring that runtime components such as OpenSSL, BusyBox, glibc, and systemd remain secure. **Key Mitigation Strategies:**

1. Upgrade base OS image (e.g., UBI 9.6, OEL 9).
2. Apply OS-level security updates using dnf/yum package manager.
3. Rebuild application runtime layers on top of the patched OS.
4. Ensure no legacy build tools or insecure utilities remain in the image.
5. Validate that backported fixes (common in RHEL/OEL ecosystems) are applied.



CVE ID	Component	Mitigation	Resolved In
CVE-2024-3094	xz-utils	Patched via UBI 9.6 update	UBI 9.6
CVE-2024-6387	OpenSSH	OS security patch applied	UBI 9.5+
CVE-2024-0727	glibc	Updated dynamic loader libs	glibc 2.34+
CVE-2023-0464	OpenSSL	Patched OpenSSL during rebuild	OpenSSL 3.0.7+