Checkmarx

April 2024 | Top 3 Docker Pitfalls

Threat Trends to Watch

In April, the Checkmarx Security Research Team analyzed 1.5 milliion results from Checkmarx One and Keeping Infrastucture-as-Code Secure(KICS) and identified three common Docker misconfigurations that threat actors can exploit.

Trend 01

58.47% - Inadvertant misconfiguration risk

Misconfigurations in Docker environments, like open network ports, weak access controls, or improper container isolation, can expose the system to threats. This can happen due to human error or oversight, which increases the likelyhood of a successful attack.

In April, we noticed that the top misconfigurations were related to a lack of validations for installed packages. For example, the usage of open versions, and lack of version pinning, which could lead to supply chain issues like dependency confusion. We also saw some misconfigurations could lead to availability issues that safeguard the operability of the container.

Accidental misconfigurations are a persistent challenge in containerized environments, often resulting from the complexity of Docker configurations and the rapid pace of deployment in modern development workflows.

It's recommended that organizations perform regular audits and use automated tools such as static code analysis to identify and remediate misconfigurations before they can be exploited by malicious actors. Additionally, security training and awareness programs can help educate developers and engineers about best practices for securely configuring and managing Docker environments.

Explore these blog posts for more information:

- How to Use Infrastructure-as-Code Securely and Avoid Cloud Misconfigurations
- A Developer's List of Key Container Security Risks
- Introducing AI-guided Remediation for IaC Security / KICS

Trend 02

23.68%: Elevated default privilges

Docker containers often run with elevated default privleges, granting them unnecessary access to system resources. This can pose a significant security risk as attackers may exploit vulnerabilities within the container or host system to gain unauthorized access or escalate privileges.

Default privileges are a common pitfall in Docker deployments. It results from default settings or configurations that prioritize functionality over security. Based on the analyzed data, we saw a visible trend where Docker images are being run with root permissions, leaving them at risk for potential access to the host machine (isolation breakdown).

It's recommended that organizations adopt a least privilege principle, ensuring that containers only have the access necessary for their intended functions. Regular security assessments and updates are also crucial to identify and address vulnerabilities that could be exploited to compromise containerized environments.

For more details and checklists, check out these resources:

- A Developer's List of Key Container Security Risks
- Code-to-Cloud Security: The Definitive Checklist for AppSec Leaders

Trend 03

17.85%: Exposure of passwords and secrets

Sensitive information, like passwords, API keys, or cryptograpic keys, can be accidently included in Docker images or configurations. When that happens, it leaves those images or configurations vulnerable to unauthorized access or extraction by threat actors.

This occurs due to oversight during the development and deployment stages. When these secrets are inserted in Docker images, they become easily accessible to anyone with access to the image, potentially leading to data breaches or unauthorized access to critical systems.

It's recommended that organizations prioritize strong security practices, including secure code review, appropriate handling of sensitive information, and usage of automated tools such as static code analysis to help detect and prevent the exposure of passwords and secrets in Docker images. When integrated into CI/CD pipelines, this enables proactive identification and mitigation of potential passwords and secrets exposures before deployment.

For more details and checklists, check out these resources:

- How to Prevent Secrets from Leaking out of Your Dev Pipeline
- Secrets, Secrets Are No Fun. Secrets, Secrets (Stored in Plain Text Files) Hurt Someone