Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Leaky Vessels in Cloud Environments Shake Docker and Beyond

Date of Publication	Admiralty Code	TA Number
February 2, 2023	A1	TA2024043

Summary

First Seen: November 20, 2023
Affected Components: Runc and BuildKit
Affected Vendors: Docker, Kubernetes, and cloud container services
Impact: Four vulnerabilities, collectively termed 'Leaky Vessels,' have been uncovered within container engine components, specifically affecting the runC command line tool. In the most severe instances, illicit entry into the underlying host operating system could result in the compromise of vital credentials, empowering adversaries to launch additional attacks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-21626	runC Security features bypass vulnerability	runc: 1.0.0 rc93 - 1.1.11	✗	✗	✓
CVE-2024-23651	BuildKit Race condition	BuildKit: 0.3.0 - 0.12.4	✗	✗	✓
CVE-2024-23652	BuildKit Path traversal Vulnerability	BuildKit: 0.3.0 - 0.12.4	✗	✗	✓
CVE-2024-23653	BuildKit Privilege escalation Vulnerability	BuildKit: 0.3.0 - 0.12.4	✗	✗	✓

Vulnerability Details

#1

A set of four vulnerabilities has been discovered within the components of container engine systems in the runC command line tool. This exposes an exploitable opportunity for malicious actors to breach containers and carry out subsequent attacks. These vulnerabilities, labeled CVE-2024-21626, CVE-2024-23651, CVE-2024-23652, and CVE-2024-23653, collectively go by the name "Leaky Vessels."

#2

In the worst-case scenarios, an unauthorized intruder gaining access to the underlying host operating system could potentially infiltrate any other processes operating on the same host. This includes but is not limited to, critical credentials that empower the adversary to launch additional attacks. One of the most severe flaws is CVE-2024-21626, impacting runC and capable of facilitating a container escape centered around the 'WORKDIR' command. runC is a tool designed for initiating and managing containers on Linux, initially part of Docker and subsequently separated into a standalone open-source library in 2015.

#3

The remaining three vulnerabilities are related to BuildKit, Docker's default toolkit for constructing container images. One of these vulnerabilities (CVE-2024-23651) involves a race condition related to the mounting of cache layers during runtime. Another (CVE-2024-23653) affects a security model within BuildKit's remote procedure call protocol, while the third vulnerability (CVE-2024-23652) is a flaw related to file deletion, also within BuildKit.

#4

Considering that these vulnerabilities impact any individual employing containers for application development, virtually every cloud-native developer globally is susceptible to the potential compromise of entire Docker or Kubernetes host systems. Independent advisories from vendors supplying container runtime environments have also issued alerts, urging customers to take necessary actions promptly.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-21626	runc: 1.0.0 rc93 - 1.1.11	cpe:2.3:a:linuxfoundation:runc:*:*:*:*:*:*:*:*	CWE-668 CWE-403
CVE-2024-23651	BuildKit: 0.3.0 - 0.12.4	cpe:2.3:a:mobyproject:buildkit:*:*:*:*:*:*:*:*	CWE-362
CVE-2024-23652	BuildKit: 0.3.0 - 0.12.4	cpe:2.3:a:mobyproject:buildkit:*:*:*:*:*:*:*:*	CWE-22
CVE-2024-23653	BuildKit: 0.3.0 - 0.12.4	cpe:2.3:a:mobyproject:buildkit:*:*:*:*:*:*:*:*	CWE-863

Recommendations

Apply Official Fixes Immediately: Apply the latest patches and updates for Docker and runC to address the identified vulnerabilities (CVE-2024-21626, CVE-2024-23651, CVE-2024-23652, CVE-2024-23653).

Compliance Checks: Ensure compliance with industry-specific security standards and regulations, conducting regular checks to verify adherence to best practices.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0006 Credential Access
TA0040 Impact	T1068 Exploitation for Privilege Escalation	T1588 Obtain Capabilities	T1098 Account Manipulation
T1588.005 Exploits	T1588.006 Vulnerabilities	T1212 Exploitation for Credential Access	T1059 Command and Scripting Interpreter

Patch Details

Update runc 1.1.12 version and the Buildkit v0.12.5 release includes patches for the issue.

Links:
https://github.com/opencontainers/runc/security/advisories/GHSA-xr7r-f8xq-vfvv

https://github.com/moby/buildkit/security/advisories/GHSA-m3r6-h7wv-7xxv

https://github.com/moby/buildkit/security/advisories/GHSA-4v98-7qmw-rqr8

https://github.com/moby/buildkit/security/advisories/GHSA-wr6v-9f75-vh2g

References

https://snyk.io/blog/leaky-vessels-docker-runc-container-breakout-vulnerabilities/

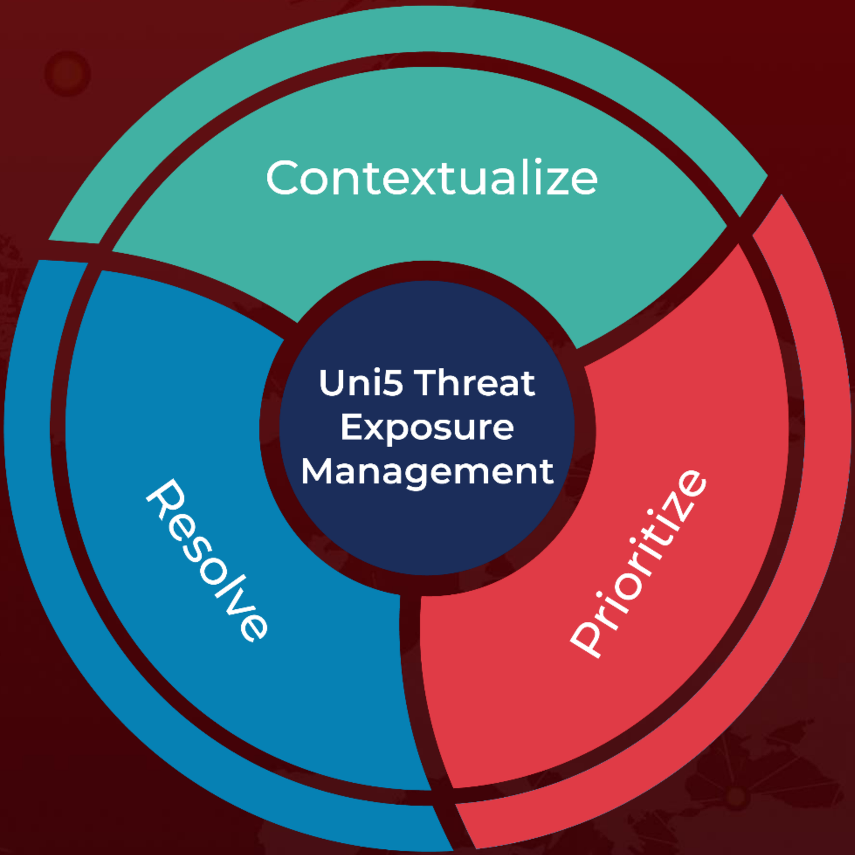
https://aws.amazon.com/security/security-bulletins/AWS-2024-001/

https://cloud.google.com/support/bulletins#gcp-2024-005

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 2, 2024 • 7:00 AM

More at www.hivepro.com