CERT-EU

Security Advisory 2024-016

High Vulnerability in the runc package

February 6, 2024 — v1.0

TLP:CLEAR

History:

- *06/02/2024 — v1.0 – Initial publication*

Summary

A critical vulnerability has been identified in all versions of **runc** package up to and including 1.1.11, affecting Docker, Kubernetes, and other containerisation technologies [1,2]. This vulnerability, tracked as `CVE-2024-21626` with a CVSS score of 8.6, enables attackers to escape containers and potentially gain unauthorised access to the host operating system.

Technical Details

The vulnerability `CVE-2024-21626` arises from an internal file descriptor leak within runc, a core component for running containers according to the Open Container Initiative (OCI) standards.

The vulnerability manifests through the improper handling of file descriptors and the `WORKDIR` directive in Dockerfiles, allowing a container process to maintain access to privileged host directory file descriptors.

Attackers can exploit this by manipulating the container's working directory to point to these file descriptors, gaining the ability to read from or write to the host filesystem.

Affected Products

This vulnerability impacts systems running runc version 1.1.11 and earlier. Due to runc's widespread use in container runtimes like Docker and Kubernetes, a significant number of containerised environments may be vulnerable.

Recommendations

CERT-EU recommends upgrading to runc version 1.1.12, which includes patches for this issue. Additionally, technologies that incorporate runc should be updated to their latest patched versions. Following vendor advisories and applying updates for container hosting services and infrastructure is also advised.

References

[1] https://snyk.io/fr/blog/cve-2024-21626-runc-process-cwd-container-breakout/

[2] https://threatprotect.qualys.com/2024/02/02/docker-patches-multiple-vulnerabilities-impacting-runc-buildkit-and-moby-leaky-vessels/

[3] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2024-21626)