CERT-EU

Security Advisory 2024-099

Critical Vulnerabilities in Openshift

September 17, 2024 — v1.0

TLP:CLEAR

History:

- *17/09/2024 — v1.0 – Initial publication*

Summary

On 16th of September 2024, two vulnerabilities (CVE-2024-45496 and CVE-2024-7387) have been discovered in Red Hat systems that allow attackers to escalate privileges or execute arbitrary code, impacting system integrity [1,2].

Technical Details

The vulnerability **CVE-2024-45496** with a CVSS score of 9.9, arises from the misuse of elevated privileges during the build process [1]. The `git-clone` container runs with privileged access, allowing attackers with developer-level permission to exploit a crafted `.gitconfig` file. This enables arbitrary command execution on the worker node. An attacker in a privileged container could escalate permission on the node, gaining unauthorised control.

The vulnerability **CVE-2024-7387** with a CVSS score of 9.1, allows command injection via path traversal. By exploiting the `spec.source.secrets.secret.destinationDir` attribute in the `BuildConfig` definition [2]. A malicious user can override executable files inside the privileged build container when using the "Docker" strategy. This leads to arbitrary command execution on the OpenShift node hosting the builder container. An attacker could use this to escalate their permission on the node, gaining unauthorised access and control.

Affected Products

- `CVE-2024-45496` : Red Hat OpenShift Container Platform 4 - `ose-openshift-controller-manager-container`
- `CVE-2024-7387` : Red Hat OpenShift Container Platform 4 - `openshift4/ose-docker-builder`

Recommendations

No specific patch is currently available. Admins should follow the instructions in [3] to block use of the "Docker" build strategy on a cluster, or restrict the use to a set of highly trusted users, until the cluster can be upgraded.

References

[1] https://access.redhat.com/security/cve/CVE-2024-45496

[2] https://access.redhat.com/security/cve/CVE-2024-7387

[3] https://docs.openshift.com/container-platform/4.16/cicd/builds/securing-builds-by-strategy.html