NCSC
National Cyber Security Centre

2409170130-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerabilities in Red Hat OpenShift Container Platform 4 (CVE-2024-45496, CVE-2024-7387)

Tuesday 17th September, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-09-17T00:15:00
Vendor: Red Hat
Product: Red Hat OpenShift Container Platform 4
CVE ID: CVE-2024-45496
CVSS3.0 Score[1]**:** 9.9
EPSS[2]**:** 0.096080000
(For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-45496)

Summary: A flaw was found in OpenShift. This issue occurs due to the misuse of elevated privileges in the OpenShift Container Platform's build process. During the build initialization step, the git-clone container is run with a privileged security context, allowing unrestricted access to the node. An attacker with developer-level access can provide a crafted .gitconfig file containing commands executed during the cloning process, leading to arbitrary command execution on the worker node. An attacker running code in a privileged container could escalate their permissions on the node running the container.

Published: 2024-09-17T00:15:00
Vendor: Red Hat
Product: Red Hat OpenShift Container Platform 4
CVE ID: CVE-2024-7387
CVSS3.0 Score: 9.1
EPSS: 0.096080000
(For up to date EPSS score, see here: https://api.first.org/data/v1/epss?cve=CVE-2024-7387)

Summary: A flaw was found in openshift/builder. This vulnerability allows command injection via path traversal, where a malicious user can execute arbitrary commands on the OpenShift node running the builder container. When using the "Docker" strategy, executable files inside the privileged build container can be overridden using the 'spec.source.secrets.secret.destinationDir' attribute of the 'BuildConfig' definition. An attacker running code in a privileged container could escalate their permissions on the node running the container.

Products Affected

- Red Hat Red Hat OpenShift Container Platform 4

Components Affected

- CVE-2024-7387: openshift4/ose-docker-builder
- CVE-2024-45496: ose-openshift-controller-manager-container

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins

Impact

Common Weakness Enumeration (CWE)[3]**:**

- CVE-2024-45496: Improper Privilege Management
- CVE-2024-7387: Execution with Unnecessary Privileges

Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** NO

Used by Ransomware Operators: Not Known

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Red Hat.

Additional recommendations and mitigation's for CVE-2024-45496 and CVE-2024-7387 can be found in the respective links below:

- https://access.redhat.com/security/cve/CVE-2024-45496
- https://access.redhat.com/security/cve/CVE-2024-7387
- https://bugzilla.redhat.com/show_bug.cgi?id=2308661

[3] https://cwe.mitre.org/

[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 K7X4,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta
Cibearshlándála
National Cyber Security Centre