Bug 2302259 (CVE-2024-7387) - CVE-2024-7387 openshift/builder: Path traversal allows command injection in privileged BuildContainer using docker build strategy

Keywords: Security

Status: NEW

Alias: CVE-2024-7387

Deadline: 2024-09-16

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2024-08-01 15:25 UTC by Michal Findra

Modified: 2024-09-19 13:25 UTC (History)

CC List: 21 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2024:6685	0	None	None	None	2024-09-19 09:30:52 UTC
Red Hat Product Errata	RHSA-2024:6687	0	None	None	None	2024-09-19 05:39:01 UTC
Red Hat	RHSA-2024:6689	0	None	None	None	2024-09-19

Product Errata						05:30:46 UTC
Red Hat Product Errata	RHSA-2024:6691	0	None	None	None	2024-09-19 00:12:40 UTC
Red Hat Product Errata	RHSA-2024:6705	0	None	None	None	2024-09-19 13:25:45 UTC

Michal Findra 2024-08-01 15:25:12 UTC Description

`OpenShift` allows a user to create his own images with the help of the build component. This component has three primary build strategies available ([Docu - Understanding image builds](https://docs.openshift.com/container-platform/4.16/cicd/builds/understanding-image-builds.html)):

* Docker build
* Source-to-Image (S2I) build
* Custom build

As the builds are running in a privileged container, a vulnerability in this process allows an attacker to escalate their permissions on the cluster and host nodes.

The `custom build` is not safe, because they can execute any code within a privileged container and are disabled by default.
The other two strategies are considered as safe and are enabled for all users that can create builds.

But there is a note about the `docker strategy`:

> Grant docker build permissions with caution, because a vulnerability in the Dockerfile processing logic could result in a privileges being granted on the host node.

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

The `docker strategy` / the image used during the build has a vulnerability, which allows an attacker to override files inside the privileged build container with the help of the `spec.source.secrets.secret.destinationDir` attribute of the `BuildConfig` definition. After overriding the binary, execution of this overriden file can be triggered with another secret and the malicious code is executed in the privileged container.

As stated above, running code in a privileged container allows an attacker to escalate their permissions on the cluster and host nodes. As an example the host filesystem of the worker node can be mounted and a new `SSH` key can be added to user `core` of the `Red Hat Enterprise Linux CoreOS (RHCOS)`.

errata-xmlrpc 2024-09-19 00:12:38 UTC Comment 1

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.13

Via RHSA-2024:6691 https://access.redhat.com/errata/RHSA-2024:6691

errata-xmlrpc 2024-09-19 05:30:44 UTC Comment 2

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.14

Via RHSA-2024:6689 https://access.redhat.com/errata/RHSA-2024:6689

errata-xmlrpc 2024-09-19 05:39:00 UTC Comment 3

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.16

Via RHSA-2024:6687 https://access.redhat.com/errata/RHSA-2024:6687

errata-xmlrpc 2024-09-19 09:30:51 UTC Comment 4

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.15

Via RHSA-2024:6685 https://access.redhat.com/errata/RHSA-2024:6685

errata-xmlrpc 2024-09-19 13:25:43 UTC Comment 5

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.12

Via RHSA-2024:6705 https://access.redhat.com/errata/RHSA-

2024:6705

Note

You need to log in before you can comment on or make changes to this bug.