مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Flaws in Red Hat OpenShift

Tracking #:432316307

Date:19-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Red Hat OpenShift, a widely used hybrid cloud platform, has been identified with two severe vulnerabilities that could potentially allow attackers to execute arbitrary commands and escalate privileges on affected nodes.

TECHNICAL DETAILS:

Red Hat OpenShift, a widely used hybrid cloud platform, has been identified with two severe vulnerabilities that could potentially allow attackers to execute arbitrary commands and escalate privileges on affected nodes. These vulnerabilities, CVE-2024-45496 and CVE-2024-7387, target the platform's build process and could pose significant risks to organizations relying on OpenShift.

Vulnerabilities Details:

1. **CVE-2024-45496**

- CVSS Score: 9.9 (Critical)
- Description: This vulnerability arises from the misuse of elevated privileges during the build initialization process. The git-clone container runs with a privileged security context, enabling attackers with developer-level access to inject malicious code through a crafted .gitconfig file, leading to arbitrary command execution on the worker node.
- Impact: Attackers can execute commands with elevated privileges on affected nodes.

2. **CVE-2024-7387**

- CVSS Score: 9.1 (Critical)
- Description: This flaw allows command injection via path traversal by exploiting the spec.source.secrets.secret.destinationDir attribute in the BuildConfig definition. Malicious users can override executable files within the privileged build container, resulting in arbitrary command execution on the node.
- Impact: Similar to CVE-2024-45496, this vulnerability allows for command execution on affected nodes.

Affected Products:

- Red Hat OpenShift Container Platform 4.13 for RHEL 9 x86_64
- Red Hat OpenShift Container Platform 4.13 for RHEL 8 x86_64
- Red Hat OpenShift Container Platform for Power 4.13 for RHEL 9 ppc64le
- Red Hat OpenShift Container Platform for Power 4.13 for RHEL 8 ppc64le
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.13 for RHEL 9 s390x
- Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.13 for RHEL 8 s390x
- Red Hat OpenShift Container Platform for ARM 64 4.13 for RHEL 9 aarch64
- Red Hat OpenShift Container Platform for ARM 64 4.13 for RHEL 8 aarch64

Fixed Version:

- Red Hat OpenShift Container Platform 4.13.50

RECOMMENDATIONS:

- Upgrade Immediately: All users of OpenShift Container Platform 4.13 should upgrade to version 4.13.50 as soon as it becomes available in the appropriate release channel.
- Restrict Build Strategies: Until patches are applied, administrators should restrict the use of the affected build strategies ("Docker" and "Source") to highly trusted users to minimize the potential for exploitation.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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