dstny Engage

Mariam Osama Saleh
9/20/2023

Analysis Results

Trivy:

- Image Information:

- Image Name: quay.io/metallb/controller:v0.13.11

- Operating System: Alpine Linux 3.18.3

- Image ID: sha256:92af1d1d71d6cf4dde3c27af4b6f259673ce4797391fce5b69058cd2d301cb8f

Vulnerability Assessment:

- Total Vulnerabilities: 0

- Image Type: Alpine Linux (alpine)

Actions:

No vulnerabilities were found in the quay.io/metallb/controller:v0.13.11 image based on the Trivy scan.

dstny Engage

Mariam Osama Saleh
9/20/2023

- Image Information:

- Image Name: longhornio/csi-attacher:v4.2.0

- Operating System: Debian 11.6

- Image ID: sha256:117b1be77e9eb708e8d632afe40e64d9d36dfd895566de23d9b712e5eea0679c

Vulnerability Assessment:

- Total Vulnerabilities: 1

Vulnerability Details:

- CVE ID: CVE-2022-41723

- Package Affected: golang.org/x/net

- Installed Version: v0.4.0

- Fixed Version: 0.7.0

- Severity: HIGH (CVSS Score: 7.5)

- Description: A maliciously crafted HTTP/2 stream could cause excessive CPU consumption in the HPACK decoder, sufficient to cause a denial of service from a small number of small requests.

- References:

  - [Red Hat Security Advisory](https://access.redhat.com/security/cve/CVE-2022-41723)

  - [CVE Details](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41723)

  - [GitHub Security Advisory](https://github.com/advisories/GHSA-vvpx-j8f3-3w6h)

Actions:

- Update the "golang.org/x/net" package to version 0.7.0 or higher to mitigate the high-severity vulnerability (CVE-2022-41723).

dstny Engage

Mariam Osama Saleh
9/20/2023

- Image Information:

- Image Name: rancher/hardened-coredns:v1.10.1-build20230406

- Operating System: SUSE Linux Enterprise Server 15.4

- Image ID: sha256:3c8207b045e329fc747a900f7bc32663b1d146909b489b1813e2fff5990daa11

Vulnerability Assessment:

- Total Vulnerabilities: 4

Vulnerability Details:

1. CVE ID: SUSE-SU-2023:3454-1

   - Package Affected: ca-certificates-mozilla

   - Installed Version: 2.60-150200.27.1

   - Fixed Version: 2.62-150200.30.1

   - Severity: UNKNOWN

   - Description: This update for ca-certificates-mozilla fixes several issues, including updating to the 2.62 state of Mozilla SSL root CAs. It adds and removes various certificates.

   - References: [SUSE Advisory](https://www.suse.com/support/update/announcement/2023/suse-su-20233454-1/)

2. CVE ID: SUSE-SU-2023:1851-1

   - Package Affected: container-suseconnect

   - Installed Version: 2.4.0-150000.4.24.1

   - Fixed Version: 2.4.0-150000.4.26.1

   - Severity: UNKNOWN

   - Description: This update for container-suseconnect fixes issues by rebuilding it against the current Go version.

- References: [SUSE Advisory](https://www.suse.com/support/update/announcement/2023/suse-su-20231851-1/)

3. CVE ID: SUSE-SU-2023:2174-1

- Package Affected: container-suseconnect

- Installed Version: 2.4.0-150000.4.24.1

- Fixed Version: 2.4.0-150000.4.28.1

- Severity: UNKNOWN

- Description: This update of container-suseconnect fixes issues by rebuilding the package with the Go 1.9 secure release.

- References: [SUSE Advisory](https://www.suse.com/support/update/announcement/2023/suse-su-20232174-1/)

4. CVE ID: SUSE-SU-2023:2923-1

- Package Affected: container-suseconnect

- Installed Version: 2.4.0-150000.4.24.1

- Fixed Version: 2.4.0-150000.4.32.1

- Severity: UNKNOWN

- Description: This update of container-suseconnect fixes issues by rebuilding the package with the Go 1.20 security release.

- References: [SUSE Advisory](https://www.suse.com/support/update/announcement/2023/suse-su-20232923-1/)

Actions:

- Update the "ca-certificates-mozilla" package to version 2.62-150200.30.1 to address the vulnerabilities listed in CVE SUSE-SU-2023:3454-1.

- Update the "container-suseconnect" package to the appropriate fixed version to address the vulnerabilities listed in CVE SUSE-SU-2023:1851-1, CVE SUSE-SU-2023:2174-1, and CVE SUSE-SU-2023:2923-1.

- Image Information:

- Image Name: rancher/rancher:v2.7.6

- Operating System: SUSE Linux Enterprise Server 15.4

- Image ID: sha256:3c8207b045e329fc747a900f7bc32663b1d146909b489b1813e2fff5990daa11

Vulnerability Assessment:

- Total Vulnerabilities: 4

Vulnerability Details:

Certainly, here are the vulnerabilities presented in a report-like format:

Vulnerability Report:

CVE-2023-26484 - Incorrect Authorization in KubeVirt:

- Package Affected: kubevirt.io/kubevirt

- Installed Version: v0.54.0

- Severity: HIGH (CVSS Score: 8.2)

- Description: This vulnerability affects KubeVirt versions 0.59.0 and prior. If a malicious user takes over a Kubernetes node where virt-handler (the KubeVirt node-daemon) is running, they can misuse the virt-handler service account to modify all node specs. This can potentially lead to elevated privileges, including accessing secrets and pods on other nodes. No patches were available at the time of publication, but a workaround involves using gatekeeper to block the virt-handler service account from modifying node specs.

- References: [CVE Details](https://access.redhat.com/security/cve/CVE-2023-26484)

GHSA-qv98-3369-g364 - Arbitrary File Read Vulnerability in KubeVirt:

- Package Affected: kubevirt.io/kubevirt

- Installed Version: v0.54.0

- Fixed Version: 0.55.1

- Severity: HIGH

- Description: This vulnerability allows users with permission to create Virtual Machine Instances (VMIs) to construct VMI specs that enable them to read arbitrary files on the host. Attack vectors include improper validation of path fields in the VMI spec, using malicious links in the containerDisk, and exploiting KubeVirt's PVC hotplugging feature. Patches to fix this vulnerability are available in KubeVirt version 0.55.1.

- References: [GitHub Advisory](https://github.com/google/security-research/security/advisories/GHSA-cvx8-ppmc-78hm)

CVE-2023-28840 - Encrypted Overlay Network Vulnerability in Docker:

- Package Affected: github.com/docker/docker

- Installed Version: v20.10.7+incompatible

- Fixed Version: 20.10.24, 23.0.3

- Severity: HIGH (CVSS Score: 7.5)

- Description: This vulnerability affects Docker's Moby daemon component (dockerd) and involves encrypted overlay networks. Attackers can inject arbitrary Ethernet frames, potentially leading to a Denial of Service (DoS) attack or other escalations. Patches are available in Moby releases 20.10.24 and 23.0.3. Workarounds include closing the VXLAN port or ensuring the `xt_u32` kernel module is available on all nodes.

- References: [CVE Details](https://access.redhat.com/security/cve/CVE-2023-28840)

These vulnerabilities pose significant security risks and should be addressed promptly by updating to the fixed versions or applying the recommended workarounds. Regularly keeping software and systems up to date is crucial for maintaining security and protecting against known vulnerabilities.

dstny Engage

Mariam Osama Saleh
9/20/2023

Kube-Bench:

Kube-Bench Vulnerability Assessment Report

Total Failures: 4

Actions Required:

Node Configuration Files:

1. 4.1.1: Ensure that the kubelet service file permissions are set to 600 or more restrictive. Execute the following command on each worker node: `chmod 600 /etc/systemd/system/kubelet.service.d/10-kubeadm.conf`

2. 4.1.2: Ensure that the kubelet service file ownership is set to root:root. Run the following command on each worker node: `chown root:root /etc/systemd/system/kubelet.service.d/10-kubeadm.conf`

3. 4.1.5: Ensure that the --kubeconfig kubelet.conf file permissions are set to 600 or more restrictive. Execute: `chmod 600 /etc/kubernetes/kubelet.conf`

4. 4.1.6: Ensure that the --kubeconfig kubelet.conf file ownership is set to root:root. Run: `chown root:root /etc/kubernetes/kubelet.conf`

5. 4.1.7: Ensure that the certificate authorities file permissions are set to 600 or more restrictive. Modify file permissions with: `chmod 600 <filename>`

6. 4.1.8: Ensure that the client certificate authorities file ownership is set to root:root. Change ownership with: `chown root:root <filename>`

7. 4.1.9: If the kubelet config.yaml configuration file is being used, validate permissions are set to 600 or more restrictive. Execute: `chmod 600 /var/lib/kubelet/config.yaml`

8. 4.1.10: If the kubelet config.yaml configuration file is being used, validate file ownership is set to root:root. Run: `chown root:root /var/lib/kubelet/config.yaml`

Kubelet Configuration:

9. 4.2.7: Remove the --hostname-override argument from the KUBELET_SYSTEM_PODS_ARGS variable in the kubelet service file

`/etc/systemd/system/kubelet.service.d/10-kubeadm.conf`. Restart the kubelet service based on your system configuration.

10. 4.2.12: Configure the kubelet to use strong cryptographic ciphers such as `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256`. Modify the kubelet service file to include the appropriate `--tls-cipher-suites` parameter and restart the kubelet service.

11. 4.2.13: Decide on an appropriate level for the PodPidsLimit parameter and set it either via the --pod-max-pids command-line parameter or the PodPidsLimit configuration file setting.

There are a total of 4 failures and 7 warnings across the worker nodes. The recommended actions should be performed to enhance the security of the Kubernetes worker nodes.

dstny Engage

Mariam Osama Saleh
9/20/2023

Kube-Hunter:

Total Vulnerabilities: 0

Actions Required:

Based on the Kube-Hunter vulnerability assessment, no vulnerabilities or open services were detected in the scanned Kubernetes environment. However, it is essential to regularly perform such assessments to ensure the ongoing security of your Kubernetes cluster.

No further actions are required at this time. Please continue to monitor and periodically run security assessments to identify and address any potential vulnerabilities that may arise in the future.

This report concludes the Kube-Hunter vulnerability assessment with no identified vulnerabilities.

dstny Engage

Mariam Osama Saleh
9/20/2023

Overall Conclusion:

1. Address the identified issues from the Kube-Bench assessment to enhance the security of your Kubernetes cluster.
2. Investigate and mitigate vulnerabilities detected in container images using Trivy. Prioritize high-severity vulnerabilities.
3. Continue to monitor and periodically assess the cluster's security using tools like Kube-Hunter to stay proactive against emerging vulnerabilities.
4. Maintain a strong security posture by keeping Kubernetes components, configurations, and container images up to date and following best practices.

Remember that Kubernetes security is an ongoing process, and regular assessments and updates are crucial to ensure the continued safety of your cluster.