

Cloud Security Scan Report

Target: aws.amazon.com

AI Risk Score: 5

Recommendation: Monitor regularly

Nmap Results:

Starting Nmap 7.95 (<https://nmap.org>) at 2025-03-30 18:21 IST

Trivy Results:

DPI Anomalies: False

DPI Suggestion: No threats detected

Latest Threats:

- **CVE ID:**

Severity: Important

Category: csaf_security_advisory

Publisher: Red Hat Product Security

Summary: Red Hat Developer Hub 1.5.1 has been released.

Details: Red Hat Developer Hub (RHDH) is Red Hat's enterprise-grade, self-managed, customizable developer portal based on Backstage.io. RHDH is supported on OpenShift and other major Kubernetes clusters (AKS, EKS, GKE). The core features of RHDH include a single pane of glass, a centralized software catalog, self-service via golden path templates, and Tech Docs. RHDH is extensible by plugins.

Terms: This content is licensed under the Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>). If you distribute this content, or a modified version of it, you must provide attribution to Red Hat Inc. and provide a link to the original.

References:

- <https://access.redhat.com/errata/RHSA-2025:3374>
- <https://access.redhat.com/security/cve/CVE-2024-45338>
- <https://access.redhat.com/security/cve/CVE-2024-47068>
- <https://access.redhat.com/security/cve/CVE-2024-52798>
- <https://access.redhat.com/security/cve/CVE-2024-55565>
- <https://access.redhat.com/security/cve/CVE-2024-56201>
- <https://access.redhat.com/security/cve/CVE-2024-56326>
- <https://access.redhat.com/security/cve/CVE-2024-56334>
- <https://access.redhat.com/security/cve/CVE-2025-22150>
- <https://access.redhat.com/security/cve/CVE-2025-29775>
- <https://access.redhat.com/security/updates/classification/>
- <https://catalog.redhat.com/search?gs&searchType=containers&q=rhdh>

- <https://developers.redhat.com/rhdh/overview>
- https://docs.redhat.com/en/documentation/red_hat_developer_hub
- https://security.access.redhat.com/data/csaf/v2/advisories/2025/rhsa-2025_3374.json

• **CVE ID:**

Severity: Important

Category: csaf_security_advisory

Publisher: Red Hat Product Security

Summary: Updated images are now available for Red Hat OpenShift AI.

Details: Release of RHOAI 2.16.0 provides these changes:

Terms: This content is licensed under the Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>). If you distribute this content, or a modified version of it, you must provide attribution to Red Hat Inc. and provide a link to the original.

References:

- <https://access.redhat.com/errata/RHSA-2025:3368>
- https://docs.redhat.com/en/documentation/red_hat_openshift_ai/
- https://security.access.redhat.com/data/csaf/v2/advisories/2025/rhsa-2025_3368.json

• **CVE ID:**

Severity: Important

Category: csaf_security_advisory

Publisher: Red Hat Product Security

Summary: Logging for Red Hat OpenShift - 6.0.6

Details: Logging for Red Hat OpenShift - 6.0.6 lokistack-gateway-container: Go JOSE's Parsing Vulnerable to Denial of Service (CVE-2025-27144) logging-loki-container: Non-linear parsing of case-insensitive content in golang.org/x/net/html (CVE-2024-45338)

Terms: This content is licensed under the Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>). If you distribute this content, or a modified version of it, you must provide attribution to Red Hat Inc. and provide a link to the original.

References:

- <https://access.redhat.com/errata/RHSA-2025:3132>
- <https://access.redhat.com/security/updates/classification/#important>
- https://bugzilla.redhat.com/show_bug.cgi?id=2333122
- https://bugzilla.redhat.com/show_bug.cgi?id=2347423
- <https://issues.redhat.com/browse/LOG-6759>
- https://security.access.redhat.com/data/csaf/v2/advisories/2025/rhsa-2025_3132.json

Target: azure.microsoft.com

AI Risk Score: 4

Recommendation: Monitor regularly

Nmap Results:

Starting Nmap 7.95 (<https://nmap.org>) at 2025-03-30 18:22 IST

Trivy Results:

DPI Anomalies: False

DPI Suggestion: No threats detected

Latest Threats:

- **CVE ID:**

Severity: Important

Category: csaf_security_advisory

Publisher: Red Hat Product Security

Summary: Red Hat Developer Hub 1.5.1 has been released.

Details: Red Hat Developer Hub (RHDH) is Red Hat's enterprise-grade, self-managed, customizable developer portal based on Backstage.io. RHDH is supported on OpenShift and other major Kubernetes clusters (AKS, EKS, GKE). The core features of RHDH include a single pane of glass, a centralized software catalog, self-service via golden path templates, and Tech Docs. RHDH is extensible by plugins.

Terms: This content is licensed under the Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>). If you distribute this content, or a modified version of it, you must provide attribution to Red Hat Inc. and provide a link to the original.

References:

- <https://access.redhat.com/errata/RHSA-2025:3374>
- <https://access.redhat.com/security/cve/CVE-2024-45338>
- <https://access.redhat.com/security/cve/CVE-2024-47068>
- <https://access.redhat.com/security/cve/CVE-2024-52798>
- <https://access.redhat.com/security/cve/CVE-2024-55565>
- <https://access.redhat.com/security/cve/CVE-2024-56201>
- <https://access.redhat.com/security/cve/CVE-2024-56326>
- <https://access.redhat.com/security/cve/CVE-2024-56334>
- <https://access.redhat.com/security/cve/CVE-2025-22150>
- <https://access.redhat.com/security/cve/CVE-2025-29775>
- <https://access.redhat.com/security/updates/classification/>
- <https://catalog.redhat.com/search?gs&searchType=containers&q=rhdh>
- <https://developers.redhat.com/rhdh/overview>
- https://docs.redhat.com/en/documentation/red_hat_developer_hub
- https://security.access.redhat.com/data/csaf/v2/advisories/2025/rhsa-2025_3374.json

- **CVE ID:**

Severity: Important

Category: csaf_security_advisory

Publisher: Red Hat Product Security

Summary: Updated images are now available for Red Hat OpenShift AI.

Details: Release of RHOAI 2.16.0 provides these changes:

Terms: This content is licensed under the Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>). If you distribute this content, or a modified version of it, you must provide attribution to Red Hat Inc. and provide a link to the original.

References:

- <https://access.redhat.com/errata/RHSA-2025:3368>
- https://docs.redhat.com/en/documentation/red_hat_openshift_ai/

- https://security.access.redhat.com/data/csaf/v2/advisories/2025/rhsa-2025_3368.json
- **CVE ID:**
Severity: Important
Category: csaf_security_advisory
Publisher: Red Hat Product Security
Summary: Logging for Red Hat OpenShift - 6.0.6
Details: Logging for Red Hat OpenShift - 6.0.6 lokistack-gateway-container: Go JOSE's Parsing Vulnerable to Denial of Service (CVE-2025-27144) logging-loki-container: Non-linear parsing of case-insensitive content in golang.org/x/net/html (CVE-2024-45338)
Terms: This content is licensed under the Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>). If you distribute this content, or a modified version of it, you must provide attribution to Red Hat Inc. and provide a link to the original.
References:
 - <https://access.redhat.com/errata/RHSA-2025:3132>
 - <https://access.redhat.com/security/updates/classification/#important>
 - https://bugzilla.redhat.com/show_bug.cgi?id=2333122
 - https://bugzilla.redhat.com/show_bug.cgi?id=2347423
 - <https://issues.redhat.com/browse/LOG-6759>
 - https://security.access.redhat.com/data/csaf/v2/advisories/2025/rhsa-2025_3132.json

Target: cloud.google.com

AI Risk Score: 10

Recommendation: Immediate patching required

Nmap Results:

Starting Nmap 7.95 (<https://nmap.org>) at 2025-03-30 18:22 IST

Trivy Results:

DPI Anomalies: False

DPI Suggestion: No threats detected

Latest Threats:

- **CVE ID:**
Severity: Important
Category: csaf_security_advisory
Publisher: Red Hat Product Security
Summary: Red Hat Developer Hub 1.5.1 has been released.
Details: Red Hat Developer Hub (RHDH) is Red Hat's enterprise-grade, self-managed, customizable developer portal based on Backstage.io. RHDH is supported on OpenShift and other major Kubernetes clusters (AKS, EKS,

GKE). The core features of RHDH include a single pane of glass, a centralized software catalog, self-service via golden path templates, and Tech Docs. RHDH is extensible by plugins.

Terms: This content is licensed under the Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>). If you distribute this content, or a modified version of it, you must provide attribution to Red Hat Inc. and provide a link to the original.

References:

- <https://access.redhat.com/errata/RHSA-2025:3374>
- <https://access.redhat.com/security/cve/CVE-2024-45338>
- <https://access.redhat.com/security/cve/CVE-2024-47068>
- <https://access.redhat.com/security/cve/CVE-2024-52798>
- <https://access.redhat.com/security/cve/CVE-2024-55565>
- <https://access.redhat.com/security/cve/CVE-2024-56201>
- <https://access.redhat.com/security/cve/CVE-2024-56326>
- <https://access.redhat.com/security/cve/CVE-2024-56334>
- <https://access.redhat.com/security/cve/CVE-2025-22150>
- <https://access.redhat.com/security/cve/CVE-2025-29775>
- <https://access.redhat.com/security/updates/classification/>
- <https://catalog.redhat.com/search?gs&searchType=containers&q=rhdh>
- <https://developers.redhat.com/rhdh/overview>
- https://docs.redhat.com/en/documentation/red_hat_developer_hub
- https://security.access.redhat.com/data/csaf/v2/advisories/2025/rhsa-2025_3374.json

• **CVE ID:**

Severity: Important

Category: csaf_security_advisory

Publisher: Red Hat Product Security

Summary: Updated images are now available for Red Hat OpenShift AI.

Details: Release of RHOAI 2.16.0 provides these changes:

Terms: This content is licensed under the Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>). If you distribute this content, or a modified version of it, you must provide attribution to Red Hat Inc. and provide a link to the original.

References:

- <https://access.redhat.com/errata/RHSA-2025:3368>
- https://docs.redhat.com/en/documentation/red_hat_openshift_ai/
- https://security.access.redhat.com/data/csaf/v2/advisories/2025/rhsa-2025_3368.json

• **CVE ID:**

Severity: Important

Category: csaf_security_advisory

Publisher: Red Hat Product Security

Summary: Logging for Red Hat OpenShift - 6.0.6

Details: Logging for Red Hat OpenShift - 6.0.6 lokistack-gateway-container: Go JOSE's Parsing Vulnerable to Denial of Service (CVE-2025-27144) logging-loki-container: Non-linear parsing of case-insensitive content in golang.org/x/net/html (CVE-2024-45338)

Terms: This content is licensed under the Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>). If you distribute this content, or a modified version of it, you must provide attribution to Red Hat Inc. and provide a link to the original.

References:

- <https://access.redhat.com/errata/RHSA-2025:3132>

- <https://access.redhat.com/security/updates/classification/#important>
- https://bugzilla.redhat.com/show_bug.cgi?id=2333122
- https://bugzilla.redhat.com/show_bug.cgi?id=2347423
- <https://issues.redhat.com/browse/LOG-6759>
- https://security.access.redhat.com/data/csaf/v2/advisories/2025/rhsa-2025_3132.json