RHSA-2025:21885 - Security Advisory

Issued: 2025-11-20 Updated: 2025-11-20

Synopsis

OpenShift Compliance Operator bug fix and enhancement update

Type/Severity

Security Advisory: Important

Topic

An updated OpenShift Compliance Operator image that fixes various bugs and adds new enhancements is now available for the Red Hat OpenShift Enterprise 4 catalog.

Description

The OpenShift Compliance Operator v1.8.0 is now available.
See the documentation for bug fix information:

https://docs.redhat.com/en/documentation/openshift_container_platform/latest/html/security_and_compliance/compliance-operator#compliance-operator-release-notes

Solution

Before applying this update, make sure all previously released errata relevant to your system have been applied. For details on how to apply this update, refer to:

https://docs.openshift.com/container-platform/latest/updating/updating_a_cluster/updating-cluster-cli.html

Fixes

- CMP-3248 - Update ocp4-cis-api-server-encryption-provider-cipher check and remediation
- CMP-3553 - SSH remediations are broadly applied for RHCOS4 profile rules
- CMP-3557 - The annotations not accurate for rule ocp4-oauth-or-oauthclient-token-maxage
- CMP-3558 - Rule supporting CNTR-OS-000720 (STIG V-257560) is not available in STIG Profile
- CMP-3571 - No variable reference for rule ocp4-configure-network-policies-namespaces
- CMP-3581 - SCC `insights-runtime-extractor-scc` should be added to default allowed list of SCCs to prevent rule failure

- CMP-3582 - Missing variable reference for resource-requests-limits rules
- CMP-3591 - Suppress openshift-sdn daemonset API warnings
- CMP-3597 - The rule audit-log-forwarding-uses-tls fail even if tls enabled for clusterloggerforwarder for openshift logging operator v6.1
- CMP-3606 - The kubelet-configure-tls-cipher-suites-kubeapiserver-operator remediation is broken on permissions
- CMP-3613 - Creating ComplianceScans directly breaks deprecated profile check logic
- CMP-3731 - Bump DISA STIG to V2R3
- CMP-3733 - Bump DISA STIG to V2R3
- CMP-3767 - No variable reference for rule ocp4-audit-profile-set in metadata.annotations
- CMP-3915 - SCCs `nested-container` and `restricted-v3` should be added to default allowed list of SCCs
- CMP-3916 - SSH rules are fragile with drop-in configuration files
- CMP-3920 - Rule rhcos4-sysctl-net-core-bpf-jit-harden reports state ERROR when the autoremediations are applied

CVEs

- CVE-2024-12085
- CVE-2025-5914
- CVE-2025-6020
- CVE-2025-6965
- CVE-2025-7195
- CVE-2025-7425
- CVE-2025-8941

References

- https://access.redhat.com/security/updates/classification/

The Red Hat security contact is secalert@redhat.com. More contact details at https://access.redhat.com/security/team/contact/.