Subscriptions | Downloads | Red Hat Console | Get Support

Cookie Preferences and Opt-Out Rights
Your Choices About Cookies on this Site

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Accept default will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

Required Cookies only will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

Clearing your browser cookies may delete your cookie preferences. If you re-visit this site after clearing browser cookies, you will need to reset your preferences at that time. If you have set your browser's global privacy settings, then we recognize the global privacy settings from your browser.

Red Hat Pro

RHSA-

2025-11-20

Overview

Updated Imag

Synopsi

OpenShift

Type/Se

Security A

Topic

An update
enhancem

Descript

The Open
See the do

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/.

Red Hat

Quick Links

Help

Site Info

Related Sites

Loading

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit

© 2026 Red Hat
Privacy statement
Terms of use
All policies and guidelines
Digital accessibility
Cookie Preferences and Opt-Out Rights