



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



Red Hat F

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.

RHSA

24-11-19

Overview

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.

Updated In

Synop

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.

Importa

Type/

Security

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.

Topic

OpenSh

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".

Red Hat

Vulnerab

for each

Common
ilable

Descri

OpenSh

resource

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 preferences to "strict" and you have enabled both file system-based and snapshot-based backups for persistent volumes.

OADP

Security Fix(es) from Bugzilla:

- [encoding/gob: golang: Calling Decoder.Decode on a message which contains deeply nested structures can cause a panic due to stack exhaustion \(CVE-2024-34156\)](#)
- [containers/image: digest type does not guarantee valid type \(CVE-2024-3727\)](#)

- [net/http](#): Denial of service due to improper 100-continue handling in net/http (CVE-2024-24791)
- go/parser: golang: Calling any of the Parse functions containing deeply nested literals can cause a panic/stack exhaustion (CVE-2024-34155)
- go/build/constraint: golang: Calling Parse on a "// +build" build tag line with deeply nested expressions can cause a panic due to stack exhaustion (CVE-2024-34158)

For more details about the security issue(s), including the impact, a CVSS score, and other related information, refer to the CVE page(s) listed in the References section.

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://access.redhat.com/articles/11258>

Affected Products

- OpenShift API for Data Protection 1 for RHEL 9 x86_64
- OpenShift API for Data Protection for ARM 64 1 for RHEL 9 aarch64
- OpenShift API for Data Protection for IBM Power, little endian 1 for RHEL 9 ppc64le
- OpenShift API for Data Protection for IBM Z and LinuxONE 1 for RHEL 9 s390x









Fixes

- [BZ - 2274767](#) - CVE-2024-3727 containers/image: digest type does not guarantee valid type
- [BZ - 2295310](#) - CVE-2024-24791 net/http: Denial of service due to improper 100-continue handling in net/http
- [BZ - 2310527](#) - CVE-2024-34155 go/parser: golang: Calling any of the Parse functions containing deeply nested literals can cause a panic/stack exhaustion
- [BZ - 2310528](#) - CVE-2024-34156 encoding/gob: golang: Calling Decoder.Decode on a message which contains deeply nested structures can cause a panic due to stack exhaustion
- [BZ - 2310529](#) - CVE-2024-34158 go/build/constraint: golang: Calling Parse on a "// +build" build tag line with deeply nested expressions can cause a panic due to stack exhaustion
- [OADP-2944](#) - backup spec.resourcepolicy.kind is only respected with lower-level string
- [OADP-4803](#) - Use olm.maxOpenShiftVersion to prevent cluster upgrade to OCP v4.16 when OADP 1.3 is installed
- [OADP-3050](#) - BSLs / VSLs are not cleared when DPA CR is modified
- [OADP-3052](#) - DPA reconcile successfully on wrong VSL secret key name

- [OADP-3562](#) - Controller pod crashes when (decrypted) Azure Secret value has empty key-value pair
- [OADP-3010](#) - Velero backup.status.validationErrors field has multiple single quotes
- [OADP-3630](#) - DevFix: openshift-velero-plugin panics on imagestream backup, due to a missing secret
- [OADP-4736](#) - Volumesnapshot getting deleted by OpenShift GitOps during backup
- [OADP-5111](#) - Backups partially fails when backing up all namespaces

CVEs



- [CVE-2023-27349](#)
- [CVE-2023-37920](#)
- [CVE-2023-44431](#)
- [CVE-2023-45866](#)
- [CVE-2023-50229](#)
- [CVE-2023-50230](#)
- [CVE-2023-51580](#)
- [CVE-2023-51589](#)
- [CVE-2023-51592](#)
- [CVE-2023-51594](#)
- [CVE-2023-51596](#)
- [CVE-2024-2236](#)
- [CVE-2024-2511](#)
- [CVE-2024-3596](#)
- [CVE-2024-3727](#)
- [CVE-2024-4603](#)
- [CVE-2024-4741](#)
- [CVE-2024-5535](#)
- [CVE-2024-6232](#)
- [CVE-2024-6239](#)
- [CVE-2024-6501](#)
- [CVE-2024-6655](#)
- [CVE-2024-24791](#)
- [CVE-2024-29510](#)
- [CVE-2024-33869](#)
- [CVE-2024-33870](#)
- [CVE-2024-34155](#)
- [CVE-2024-34156](#)
- [CVE-2024-34158](#)
- [CVE-2024-34397](#)
- [CVE-2024-40866](#)
- [CVE-2024-42472](#)


- [CVE-2024-44185](#) 
- [CVE-2024-44187](#) 
- [CVE-2024-44244](#) 
- [CVE-2024-44296](#) 
- [CVE-2024-47175](#) 
- [CVE-2024-50602](#) 
- [CVE-2024-52530](#) 
- [CVE-2024-52532](#) 


References

- <https://access.redhat.com/security/updates/classification/#important> 


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




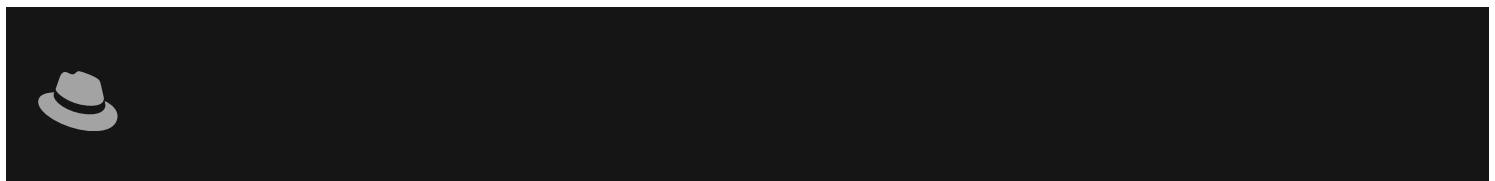
Quick Links 

Help 

Site Info 

Related Sites 

 Partial system outage



[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](#)