



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**Advis**

1-09-26

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

Importan

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.

Type/Severity

Security Advisory: Important

Topic

The Migration Toolkit for Containers (MTC) 1.8.4 is now available.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

Description

The Migration Toolkit for Containers (MTC) enables you to migrate Kubernetes resources, persistent volume data, and internal container images between OpenShift Container Platform clusters, using the MTC web console or the Kubernetes API.

Security Fix(es) from Bugzilla:

- golang: net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS (CVE-2023-45288)
- webpack-dev-middleware: lack of URL validation may lead to file leak (CVE-2024-29180)
- express: cause malformed URLs to be evaluated (CVE-2024-29041)
- axios: axios: Server-Side Request Forgery (CVE-2024-39338)
- golang: net/http/cookiejar: incorrect forwarding of sensitive headers and cookies on HTTP redirect (CVE-2023-45289)
- jose-go: improper handling of highly compressed data (CVE-2024-28180)
- follow-redirects: Possible credential leak (CVE-2024-28849)
- moby: external DNS requests from 'internal' networks could lead to data exfiltration (CVE-2024-29018)
- containers/image: digest type does not guarantee valid type (CVE-2024-3727)
- golang: net: malformed DNS message can cause infinite loop (CVE-2024-24788)
- braces: fails to limit the number of characters it can handle (CVE-2024-4068)
- node-tar: denial of service while parsing a tar file due to lack of folders depth validation (CVE-2024-28863)

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

- Red Hat Migration Toolkit 1 for RHEL 8 x86_64

Fixes

- [BZ - 2268018](#)  - CVE-2023-45289 golang: net/http/cookiejar: incorrect forwarding of sensitive headers and cookies on HTTP redirect
- [BZ - 2268273](#)  - CVE-2023-45288 golang: net/http, x/net/http2: unlimited number of CONTINUATION frames causes DoS
- [BZ - 2268854](#)  - CVE-2024-28180 jose-go: improper handling of highly compressed data
- [BZ - 2269576](#)  - CVE-2024-28849 follow-redirects: Possible credential leak
- [BZ - 2270591](#)  - CVE-2024-29018 moby: external DNS requests from 'internal' networks could lead to data exfiltration

- [BZ - 2270863](#) - CVE-2024-29180 webpack-dev-middleware: lack of URL validation may lead to file leak
- [BZ - 2274767](#) - CVE-2024-3727 containers/image: digest type does not guarantee valid type
- [BZ - 2279814](#) - CVE-2024-24788 golang: net: malformed DNS message can cause infinite loop
- [BZ - 2280600](#) - CVE-2024-4068 braces: fails to limit the number of characters it can handle
- [BZ - 2290901](#) - CVE-2024-29041 express: cause malformed URLs to be evaluated
- [BZ - 2293200](#) - CVE-2024-28863 node-tar: denial of service while parsing a tar file due to lack of folders depth validation
- [BZ - 2295302](#) - CVE-2019-25211 github.com/gin-contrib/cors: Gin mishandles a wildcard in the origin string in github.com/gin-contrib/cors
- [BZ - 2299624](#) - MigClusters showing wrong operator version in UI
- [BZ - 2299625](#) - UI stuck at "Namespaces" while creating a migplan
- [BZ - 2299628](#) - Migration stuck as DirectVolumeMigration fails with "InvalidPVCs" error
- [BZ - 2299668](#) - Migration fails with error: no matches for kind "Virtual machine" in version "kubevirt/v1"
- [MIG-1593](#) - MigClusters showing wrong operator version in UI
- [MIG-1592](#) - DVM fails when migrating to a namespace different from the source namespace
- [MIG-1598](#) - Rollback after a migration gets stuck at Quiescing step
- [MIG-1610](#) - Rollback performed after a failed migration fails at RollbackLiveMigration step

CVEs

- [CVE-2018-15209](#)
- [CVE-2019-25211](#)
- [CVE-2020-28241](#)
- [CVE-2021-43618](#)
- [CVE-2022-48468](#)
- [CVE-2022-48622](#)
- [CVE-2022-48624](#)
- [CVE-2023-2953](#)
- [CVE-2023-3446](#)
- [CVE-2023-3817](#)
- [CVE-2023-4016](#)
- [CVE-2023-5678](#)
- [CVE-2023-6004](#)
- [CVE-2023-6228](#)
- [CVE-2023-6597](#)
- [CVE-2023-6918](#)
- [CVE-2023-7104](#)

- [CVE-2023-25193](#)
- [CVE-2023-25433](#)
- [CVE-2023-43785](#)
- [CVE-2023-43786](#)
- [CVE-2023-43787](#)
- [CVE-2023-43788](#)
- [CVE-2023-43789](#)
- [CVE-2023-45288](#)
- [CVE-2023-45289](#)
- [CVE-2023-45290](#)
- [CVE-2023-52356](#)
- [CVE-2024-0450](#)
- [CVE-2024-1737](#)
- [CVE-2024-1975](#)
- [CVE-2024-2398](#)
- [CVE-2024-3651](#)
- [CVE-2024-3727](#)
- [CVE-2024-4068](#)
- [CVE-2024-6345](#)
- [CVE-2024-24783](#)
- [CVE-2024-24788](#)
- [CVE-2024-25062](#)
- [CVE-2024-28180](#)
- [CVE-2024-28182](#)
- [CVE-2024-28834](#)
- [CVE-2024-28849](#)
- [CVE-2024-28863](#)
- [CVE-2024-29018](#)
- [CVE-2024-29041](#)
- [CVE-2024-29180](#)
- [CVE-2024-32002](#)
- [CVE-2024-32004](#)
- [CVE-2024-32020](#)
- [CVE-2024-32021](#)
- [CVE-2024-32465](#)
- [CVE-2024-32487](#)
- [CVE-2024-33599](#)
- [CVE-2024-33600](#)
- [CVE-2024-33601](#)
- [CVE-2024-33602](#)

- [CVE-2024-33871](#)
- [CVE-2024-34064](#)
- [CVE-2024-35235](#)
- [CVE-2024-37370](#)
- [CVE-2024-37371](#)
- [CVE-2024-37891](#)
- [CVE-2024-38428](#)
- [CVE-2024-39331](#)
- [CVE-2024-39338](#)


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/>.



The image shows the Red Hat logo and a navigation menu. The logo consists of a red fedora hat icon and the text "Red Hat". To the right of the logo are social media icons for LinkedIn, YouTube, Facebook, and X. Below the logo is a navigation menu with four items: "Quick Links", "Help", "Site Info", and "Related Sites". Each item has a downward-pointing chevron icon to its right.

 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](#)