



# 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**

26-01-21

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**

Release

**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  
ailable

**Descri**

This rele

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

- CVE-2024-12718 python3-libs-3.8-09.el8\_10.x86\_64 python3-libs-3.8-69.el8\_10.x86\_64 RHSA-2025:10128
- CVE-2025-30749 java-17-openjdk-devel-17.0.15.0.6-2.el8.x86\_64 java-17-openjdk-17.0.15.0.6-2.el8.x86\_64 java-17-openjdk-headless-17.0.15.0.6-2.el8.x86\_64 RHSA-2025:10867
- CVE-2025-40778 python3-bind-9.11.36-16.el8\_10.4.noarch bind-license-9.11.36-16.el8\_10.4.noarch bind-libs-9.11.36-16.el8\_10.4.x86\_64 bind-libs-lite-9.11.36-16.el8\_10.4.x86\_64 bind-utils-9.11.36-16.el8\_10.4.x86\_64 RHSA-2025:19835

- CVE-2025-4138 platform-python-3.6.8-69.el8\_10.x86\_64 python3-libs-3.6.8-69.el8\_10.x86\_64 RHSA-2025:10128
- CVE-2025-4517 python3-libs-3.6.8-69.el8\_10.x86\_64 platform-python-3.6.8-69.el8\_10.x86\_64 RHSA-2025:10128
- CVE-2025-49794 libxml2-2.9.7-19.el8\_10.x86\_64 RHSA-2025:10698
- CVE-2025-49796 libxml2-2.9.7-19.el8\_10.x86\_64 RHSA-2025:10698
- CVE-2025-50059 java-17-openjdk-devel-17.0.15.0.6-2.el8.x86\_64 java-17-openjdk-17.0.15.0.6-2.el8.x86\_64 java-17-openjdk-headless-17.0.15.0.6-2.el8.x86\_64 RHSA-2025:10867
- CVE-2025-50106 java-17-openjdk-devel-17.0.15.0.6-2.el8.x86\_64, java-17-openjdk-17.0.15.0.6-2.el8.x86\_64 java-17-openjdk-headless-17.0.15.0.6-2.el8.x86\_64 RHSA-2025:10867
- CVE-2025-58060 cups-libs-2.2.6-62.el8\_10.x86\_64 RHSA-2025:15702
- CVE-2025-5914 libarchive-3.3.3-5.el8.x86\_64 RHSA-2025:14135
- CVE-2025-59375 expat-2.2.5-17.el8\_10.x86\_64 RHSA-2025:21776
- CVE-2025-6020 pam-1.3.1-36.el8\_10.x86\_64 RHSA-2025:10027
- CVE-2025-6965 sqlite-libs-3.26.0-19.el8\_9.x86\_64 RHSA-2025:12010
- CVE-2025-7425 libxml2-2.9.7-19.el8\_10.x86\_64 RHSA-2025:12450
- CVE-2025-8941 pam-1.3.1-36.el8\_10.x86\_64 RHSA-2025:14557

## 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 OpenShift Serverless 1 for RHEL 8 x86\_64
- Red Hat OpenShift Serverless for IBM Power, little endian 1 for RHEL 8 ppc64le
- Red Hat OpenShift Serverless for IBM Z and LinuxONE 1 for RHEL 8 s390x
- Red Hat OpenShift Serverless for ARM 1 for RHEL 8 aarch64

## Fixes

- BZ - 2370013  - CVE-2024-12718 cpython: python: Bypass extraction filter to modify file metadata outside extraction directory
- BZ - 2370016  - CVE-2025-4517 python: cpython: Arbitrary writes via tarfile realpath overflow
- BZ - 2370861  - CVE-2025-5914 libarchive: Double free at archive\_read\_format\_rar\_seek\_data() in archive\_read\_support\_format\_rar.c
- BZ - 2372373  - CVE-2025-49794 libxml: Heap use after free (UAF) leads to Denial of service (DoS)

- [BZ - 2372385](#) - CVE-2025-49796 libxml: Type confusion leads to Denial of service (DoS)
- [BZ - 2372426](#) - CVE-2025-4138 cpython: python: Bypassing extraction filter to create symlinks to arbitrary targets outside extraction directory
- [BZ - 2372512](#) - CVE-2025-6020 linux-pam: Linux-pam directory Traversal
- [BZ - 2376783](#) - CVE-2025-30749 openjdk: Better Glyph drawing (Oracle CPU 2025-07)
- [BZ - 2376785](#) - CVE-2025-50059 openjdk: Improve HTTP client header handling (Oracle CPU 2025-07)
- [BZ - 2379031](#) - CVE-2025-50106 openjdk: Glyph out-of-memory access and crash (Oracle CPU 2025-07)
- [BZ - 2379274](#) - CVE-2025-7425 libxslt: Heap Use-After-Free in libxslt caused by atype corruption in xmlAttrPtr
- [BZ - 2380149](#) - CVE-2025-6965 sqlite: Integer Truncation in SQLite
- [BZ - 2388220](#) - CVE-2025-8941 linux-pam: Incomplete fix for CVE-2025-6020
- [BZ - 2392595](#) - CVE-2025-58060 cups: Authentication Bypass in CUPS Authorization Handling
- [BZ - 2395108](#) - CVE-2025-59375 expat: libexpat in Expat allows attackers to trigger large dynamic memory allocations via a small document that is submitted for parsing
- [BZ - 2405827](#) - CVE-2025-40778 bind: Cache poisoning attacks with unsolicited RRs

## CVEs

- [CVE-2013-0340](#)
- [CVE-2016-9840](#)
- [CVE-2019-17543](#)
- [CVE-2022-23990](#)
- [CVE-2023-40403](#)
- [CVE-2024-12718](#)
- [CVE-2024-28757](#)
- [CVE-2024-34397](#)
- [CVE-2024-47081](#)
- [CVE-2024-52533](#)
- [CVE-2024-53920](#)
- [CVE-2025-3576](#)
- [CVE-2025-4138](#)
- [CVE-2025-4330](#)
- [CVE-2025-4373](#)
- [CVE-2025-4435](#)
- [CVE-2025-4517](#)
- [CVE-2025-4802](#)
- [CVE-2025-5318](#)
- [CVE-2025-5372](#)
- [CVE-2025-5914](#)

- [CVE-2025-6020](#)
- [CVE-2025-6021](#)
- [CVE-2025-6395](#)
- [CVE-2025-6965](#)
- [CVE-2025-7425](#)
- [CVE-2025-8058](#)
- [CVE-2025-8194](#)
- [CVE-2025-8941](#)
- [CVE-2025-30749](#)
- [CVE-2025-32414](#)
- [CVE-2025-32415](#)
- [CVE-2025-32988](#)
- [CVE-2025-32990](#)
- [CVE-2025-40778](#)
- [CVE-2025-40909](#)
- [CVE-2025-47151](#)
- [CVE-2025-47273](#)
- [CVE-2025-47947](#)
- [CVE-2025-49794](#)
- [CVE-2025-49796](#)
- [CVE-2025-50059](#)
- [CVE-2025-50106](#)
- [CVE-2025-53057](#)
- [CVE-2025-53066](#)
- [CVE-2025-53905](#)
- [CVE-2025-53906](#)
- [CVE-2025-58060](#)
- [CVE-2025-58364](#)
- [CVE-2025-59375](#)

## References

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

---

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



Quick Links



Help



Site Info



Related Sites



✔ All systems operational



[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