



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

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.

Overview

Updated P

Synop

Moderat

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: Moderate

I-08-07

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#)

Topic

An update for libtiff is now available for Red Hat Enterprise Linux 8.

Red Hat Product Security has rated this update as having a security impact of Moderate. 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 libtiff packages contain a library of functions for manipulating Tagged Image File Format (TIFF) files.

Security Fix(es):

- libtiff: Heap-based buffer overflow in ChopUpSingleUncompressedStrip in tif_dirread.c (CVE-2018-15209)
- libtiff: Buffer Overflow via /libtiff/tools/tiffcrop.c (CVE-2023-25433)
- libtiff: heap-based buffer overflow in cpStripToTile() in tools/tiffcp.c (CVE-2023-6228)
- libtiff: Segment fault in libtiff in TIFFReadRGBATileExt() leading to denial of service (CVE-2023-52356)

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

Solution



For details on how to apply this update, which includes the changes described in this advisory, refer to:

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

Affected Products

- Red Hat Enterprise Linux for x86_64 8 x86_64
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat CodeReady Linux Builder for x86_64 8 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le
- Red Hat CodeReady Linux Builder for ARM 64 8 aarch64
- Red Hat CodeReady Linux Builder for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x

Fixes

- [BZ - 1614051](#)  - CVE-2018-15209 libtiff: Heap-based buffer overflow in ChopUpSingleUncompressedStrip in tif_dirread.c
- [BZ - 2218744](#)  - CVE-2023-25433 libtiff: Buffer Overflow via /libtiff/tools/tiffcrop.c

- [BZ - 2240995](#) - CVE-2023-6228 libtiff: heap-based buffer overflow in cpStripToTile() in tools/tiffcp.c
- [BZ - 2251344](#) - CVE-2023-52356 libtiff: Segment fault in libtiff in TIFFReadRGBATileExt() leading to denial of service

CVEs

- [CVE-2018-15209](#)
- [CVE-2023-6228](#)
- [CVE-2023-25433](#)
- [CVE-2023-52356](#)

References

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

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



 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](#)