

[Red Hat Product Errata](#)    [RHSA-2025:17740 - Security Advisory](#)

# RHSA-2025:17740 - Security Advisory

 Issued: 2025-10-13    Updated: 2025-10-13[Overview](#)[Updated Packages](#)

## Synopsis

Important: compat-libtiff3 security update

## Type/Severity

Security Advisory: Important

### Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

## Topic

An update for compat-libtiff3 is now available for Red Hat Enterprise Linux 8.8 Update Services for SAP Solutions and Red Hat Enterprise Linux 8.8 Telecommunications Update Service.

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 libtiff3 package provides libtiff 3, an older version of libtiff library for manipulating TIFF (Tagged Image File Format) image format files. This version should be used only if you are unable to use the current version of libtiff.

Security Fix(es):

- libtiff: Libtiff Write-What-Where (CVE-2025-9900)

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 - Extended Update Support Extension 8.8 x86\_64
- Red Hat Enterprise Linux Server - TUS 8.8 x86\_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 8.8 x86\_64

## Fixes

- [BZ - 2392784](#)  - CVE-2025-9900 libtiff: Libtiff Write-What-Where

## CVEs

- [CVE-2025-9900](#) 

## 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 Do Not Sell or Share My Personal Information