CVE-2025-9900

VEX

Public on September 22, 2025
Last modified: November 7, 2025 at 9:35:54 PM UTC

IMPORTANT

Important severity
What does this mean?

8.8

CVSS v3 Score Breakdown

Jump to section

cription Statement Mitigation Additional information Affected Packages CVSS Score Details Weakness (CWE) Acknowledgements

Description

A flaw was found in Libtiff. This vulnerability is a "write-what-where" condition, triggered when the library processes a specially crafted TIFF image file.

By providing an abnormally large image height value in the file's metadata, an attacker can trick the library into writing attacker-controlled color data to an arbitrary memory location. This memory corruption can be exploited to cause a denial of service (application crash) or to achieve arbitrary code execution with the permissions of the user.

Statement

This attack requires user interaction to run the malicious TIFF image file, hence the CVE is maintained as important.

Mitigation

Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

Additional information

- Bugzilla 2392784: libtiff: Libtiff Write-What-Where
- CWE-123: Write-what-where Condition

External references

- https://www.cve.org/CVERecord?id=CVE-2025-9900
- https://nvd.nist.gov/vuln/detail/CVE-2025-9900
- https://github.com/SexyShoelessGodofWar/LibTiff-4.7.0-Write-What-Where?tab=readme-ov-file
- https://gitlab.com/libtiff/libtiff/-/issues/704
- https://gitlab.com/libtiff/libtiff/-/merge_requests/732
- https://libtiff.gitlab.io/libtiff/releases/v4.7.1.html

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services | Components | State | Errata

Clear all

Products / Services	Red Hat Enterprise Linux 10
Components	libtiff
State	Fixed
Justification	None
Errata	RHSA-2025:19156

Release Date	October 28, 2025

Products / Services	Red Hat Enterprise Linux 10
Components	libtiff
State	Fixed
Justification	None
Errata	RHSA-2025:20998
Release Date	November 11, 2025

Products / Services	Red Hat Enterprise Linux 7 Extended Lifecycle Support

1-10 of 41

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

CVSS v3 Score Breakdown

	Red Hat	NVD
CVSS v3 Base Score	8.8	N/A
Attack Vector	Network	N/A

	Red Hat	NVD
Attack Complexity	Low	N/A
Privileges Required	None	N/A
User Interaction	Required	N/A
Scope	Unchanged	N/A
Confidentiality Impact	High	N/A
Integrity Impact	High	N/A
Availability Impact	High	N/A

CVSS v3 Vector

Red Hat: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Acknowledgements

Red Hat would like to thank Gareth C (AnchorSec Ltd.) for reporting this issue.

Frequently Asked Questions

- Why is Red Hat's CVSS v3 score or Impact different from other vendors? >
- My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability? >
- What can I do if my product is listed as "Will not fix"? >
- What can I do if my product is listed as "Fix deferred"? >
- What is a mitigation? >

I have a Red Hat product but it is not in the above list, is it affected?

Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?

My product is listed as "Out of Support Scope". What does this mean?

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: November 7, 2025 at 9:35:54 PM UTC