Bug 2392784 (CVE-2025-9900) - CVE-2025-9900 libtiff: Libtiff Write-What-Where

Keywords: Security ×

Status: NEW

Alias: CVE-2025-9900

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2423626 2423627 2423628 2423629 2423631 2423632 2423633 2423634 ~~2423630~~

Blocks:

TreeView+ depends on / blocked

Reported: 2025-09-03 03:01 UTC by OSIDB Bzimport

Modified: 2026-03-11 03:07 UTC (History)

CC List: 1 user (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHBA-2025:19527	0	None	None	None	2025-11-03 22:19:49 UTC
Red Hat Product Errata	RHSA-2025:17651	0	None	None	None	2025-10-09 08:06:43 UTC

Red Hat Product Errata	RHSA-2025:17675	0	None	None	None	2025-10-09 10:48:03 UTC
Red Hat Product Errata	RHSA-2025:17710	0	None	None	None	2025-10-09 18:44:26 UTC
Red Hat Product Errata	RHSA-2025:17738	0	None	None	None	2025-10-13 01:18:39 UTC
Red Hat Product Errata	RHSA-2025:17739	0	None	None	None	2025-10-13 01:21:02 UTC
Red Hat Product Errata	RHSA-2025:17740	0	None	None	None	2025-10-13 01:18:17 UTC
Red Hat Product Errata	RHSA-2025:19113	0	None	None	None	2025-10-28 00:16:08 UTC
Red Hat Product Errata	RHSA-2025:19156	0	None	None	None	2025-10-28 08:38:14 UTC
Red Hat Product Errata	RHSA-2025:19276	0	None	None	None	2025-10-29 23:01:53 UTC
Red Hat Product Errata	RHSA-2025:19906	0	None	None	None	2025-11-06 11:15:13 UTC
Red Hat Product Errata	RHSA-2025:19947	0	None	None	None	2025-11-10 02:17:37 UTC
Red Hat Product Errata	RHSA-2025:20956	0	None	None	None	2025-11-11 14:59:48 UTC
Red Hat Product Errata	RHSA-2025:20998	0	None	None	None	2025-11-11 19:12:12 UTC
Red Hat Product Errata	RHSA-2025:21060	0	None	None	None	2025-11-12 02:34:44 UTC
Red Hat	RHSA-2025:21061	0	None	None	None	2025-11-12

Product Errata						02:30:58 UTC
Red Hat Product Errata	RHSA-2025:21062	0	None	None	None	2025-11-12 02:38:17 UTC
Red Hat Product Errata	RHSA-2025:21407	0	None	None	None	2025-11-17 01:17:00 UTC
Red Hat Product Errata	RHSA-2025:21506	0	None	None	None	2025-11-17 11:35:18 UTC
Red Hat Product Errata	RHSA-2025:21507	0	None	None	None	2025-11-17 12:01:10 UTC
Red Hat Product Errata	RHSA-2025:21508	0	None	None	None	2025-11-17 11:57:17 UTC
Red Hat Product Errata	RHSA-2026:0001	0	None	None	None	2026-01-05 00:47:39 UTC
Red Hat Product Errata	RHSA-2026:0076	0	None	None	None	2026-01-05 17:56:31 UTC
Red Hat Product Errata	RHSA-2026:0077	0	None	None	None	2026-01-05 18:04:51 UTC
Red Hat Product Errata	RHSA-2026:0078	0	None	None	None	2026-01-05 17:38:11 UTC

OSIDB Bzimport 2025-09-03 03:01:18 UTC Description

```
Write-What-Where in libtiff via TIFFReadRGBAImageOriented

The vulnerability resides in the raster decoding logic of
libtiff, specifically when processing paletted (indexed color)
images with malformed metadata. The function
TIFFReadRGBAImageOriented() computes a pointer offset into the
raster buffer based on user-controlled image metadata:

raster + (rheight - img.height) * rwidth

If the attacker supplies a very large value for img.height
(e.g., 0xFFFF) and a valid rheight (e.g., 256), this
computation results in a large positive offset, causing the
raster pointer (cp) passed into functions like
put8bitcmaptile() or put1bitbwtile() to point beyond the
```

bounds of the allocated buffer.

Inside those functions, memory writes occur like this:

*cp++ = PALmap[*pp][0];

• The write address (cp) is attacker-controlled via the offset calculation from img.height.
• The value written (PALmap[*pp][0]) is also attacker-controlled:
    ◦ *pp is dereferenced from pixel data in the image file.
    ◦ PALmap is constructed from the image's color palette, which the attacker also controls.
This constitutes a write-what-where vulnerability with a attacker control. Exploitation of a write-what-where primitive can lead to denial of service or code execution through supply of maliciously crafted files.

errata-xmlrpc 2025-10-09 08:06:42 UTC Comment 2

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support
  Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On

Via RHSA-2025:17651 https://access.redhat.com/errata/RHSA-2025:17651

errata-xmlrpc 2025-10-09 10:48:02 UTC Comment 3

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2025:17675 https://access.redhat.com/errata/RHSA-2025:17675

errata-xmlrpc 2025-10-09 18:44:25 UTC Comment 4

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 7 Extended Lifecycle Support

Via RHSA-2025:17710 https://access.redhat.com/errata/RHSA-2025:17710

errata-xmlrpc 2025-10-13 01:18:16 UTC Comment 5

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.8 Update Services for SAP Solutions
  Red Hat Enterprise Linux 8.8 Telecommunications Update Service

Via RHSA-2025:17740 https://access.redhat.com/errata/RHSA-2025:17740

errata-xmlrpc 2025-10-13 01:18:38 UTC Comment 6

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.2 Advanced Update Support

Via RHSA-2025:17738 https://access.redhat.com/errata/RHSA-2025:17738

errata-xmlrpc 2025-10-13 01:21:01 UTC Comment 7

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support
  Red Hat Enterprise Linux 8.6 Update Services for SAP Solutions
  Red Hat Enterprise Linux 8.6 Telecommunications Update Service

Via RHSA-2025:17739 https://access.redhat.com/errata/RHSA-2025:17739

errata-xmlrpc 2025-10-28 00:16:07 UTC Comment 8

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2025:19113 https://access.redhat.com/errata/RHSA-2025:19113

errata-xmlrpc 2025-10-28 08:38:14 UTC Comment 9

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 10

Via RHSA-2025:19156 https://access.redhat.com/errata/RHSA-2025:19156

errata-xmlrpc 2025-10-29 23:01:51 UTC Comment 10

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2025:19276 https://access.redhat.com/errata/RHSA-2025:19276

errata-xmlrpc 2025-11-06 11:15:12 UTC Comment 11

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2025:19906 https://access.redhat.com/errata/RHSA-2025:19906

errata-xmlrpc 2025-11-10 02:17:36 UTC Comment 12

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.8 Update Services for SAP Solutions
  Red Hat Enterprise Linux 8.8 Telecommunications Update Service

Via RHSA-2025:19947 https://access.redhat.com/errata/RHSA-2025:19947

errata-xmlrpc 2025-11-11 14:59:46 UTC Comment 13

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2025:20956 https://access.redhat.com/errata/RHSA-

2025:20956

errata-xmlrpc 2025-11-11 19:12:10 UTC Comment 14

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 10

Via RHSA-2025:20998 https://access.redhat.com/errata/RHSA-2025:20998

errata-xmlrpc 2025-11-12 02:30:57 UTC Comment 15

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support
  Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On

Via RHSA-2025:21061 https://access.redhat.com/errata/RHSA-2025:21061

errata-xmlrpc 2025-11-12 02:34:43 UTC Comment 16

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support
  Red Hat Enterprise Linux 8.6 Update Services for SAP Solutions
  Red Hat Enterprise Linux 8.6 Telecommunications Update Service

Via RHSA-2025:21060 https://access.redhat.com/errata/RHSA-2025:21060

errata-xmlrpc 2025-11-12 02:38:16 UTC Comment 17

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.2 Advanced Update Support

Via RHSA-2025:21062 https://access.redhat.com/errata/RHSA-

2025:21062

errata-xmlrpc 2025-11-17 01:16:59 UTC Comment 18

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 7 Extended Lifecycle Support

Via RHSA-2025:21407 https://access.redhat.com/errata/RHSA-2025:21407

errata-xmlrpc 2025-11-17 11:35:17 UTC Comment 19

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2025:21506 https://access.redhat.com/errata/RHSA-2025:21506

errata-xmlrpc 2025-11-17 11:57:16 UTC Comment 20

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.2 Update Services for SAP Solutions

Via RHSA-2025:21508 https://access.redhat.com/errata/RHSA-2025:21508

errata-xmlrpc 2025-11-17 12:01:09 UTC Comment 21

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2025:21507 https://access.redhat.com/errata/RHSA-2025:21507

errata-xmlrpc 2026-01-05 00:47:38 UTC Comment 22

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.8 Update Services for SAP Solutions
  Red Hat Enterprise Linux 8.8 Telecommunications Update Service

Via RHSA-2026:0001 https://access.redhat.com/errata/RHSA-2026:0001

errata-xmlrpc 2026-01-05 17:38:10 UTC Comment 23

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.2 Advanced Update Support

Via RHSA-2026:0078 https://access.redhat.com/errata/RHSA-2026:0078

errata-xmlrpc 2026-01-05 17:56:29 UTC Comment 24

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support
  Red Hat Enterprise Linux 8.6 Update Services for SAP Solutions
  Red Hat Enterprise Linux 8.6 Telecommunications Update Service

Via RHSA-2026:0076 https://access.redhat.com/errata/RHSA-2026:0076

errata-xmlrpc 2026-01-05 18:04:49 UTC Comment 25

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support
  Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On

Via RHSA-2026:0077 https://access.redhat.com/errata/RHSA-2026:0077

Note

You need to log in before you can comment on or make changes to this bug.