



# CVE-2023-0799

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-0799
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@gitlab.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-02-13 23:15:00 UTC
<b>Updated</b>	2023-05-30 06:16:00 UTC
<b>Description</b>	LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3701, allowing attackers to cause a denial-of-service vi

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libtiff	Libtiff	All	All	All	All

## References

Reference	Source	Link
Debian -- Security Information -- DSA-5361-1 tiff	DEBIAN	<a href="#">www.de</a>
March 2023 LibTIFF Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security</a>
2023/CVE-2023-0799.json · master · GitLab.org / cves · GitLab	CONFIRM	<a href="#">gitlab.c</a>
[SECURITY] [DLA 3333-1] tiff security update	MLIST	<a href="#">lists.del</a>
LibTIFF: Multiple Vulnerabilities (GLSA 202305-31) — Gentoo security	GENTOO	<a href="#">security</a>
tiffcrop: heap-use-after-free in extractContigSamplesShifted32bits, tiffcrop.c:3701 (#494) · Issues · libtiff / libtiff · GitLab	MISC	<a href="#">gitlab.c</a>
Merge branch 'tiffcrop_R270_fix#492' into 'master' (afaabc3e) · Commits · libtiff / libtiff · GitLab	MISC	<a href="#">gitlab.c</a>
CVE Program record	CVE.ORG	<a href="#">www.cv</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nis</a>

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** wangdw.augustus@gmail.com

## Legacy QID Mappings

[160748](#) Oracle Enterprise Linux Security Update for libtiff (ELSA-2023-3711)

[181600](#) Debian Security Update for tiff (DLA 3333-1)

[181682](#) Debian Security Update for tiff (DSA 5361-1)

[183493](#) Debian Security Update for tiff (CVE-2023-0799)

[199216](#) Ubuntu Security Notification for LibTIFF Vulnerabilities (USN-5923-1)

[241737](#) Red Hat Update for libtiff (RHSA-2023:3711)

[502796](#) Alpine Linux Security Update for tiff

[503026](#) Alpine Linux Security Update for tiff

[503134](#) Alpine Linux Security Update for tiff

[503693](#) Alpine Linux Security Update for tiff

[505947](#) Alpine Linux Security Update for tiff

[672867](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-1599)

[672968](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-1874)

[672998](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-1849)

[673036](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-1957)

[673055](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-1979)

[673076](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-2157)

[673143](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-2298)

[673160](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-2274)

[710734](#) Gentoo Linux LibTIFF Multiple Vulnerabilities (GLSA 202305-31)

[754055](#) SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2023:2321-1)

[754062](#) SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2023:2334-1)

[905497](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13382)

[905501](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13394)

[906313](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13394-1)

[906516](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13394-2)

[906555](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13382-1)

[906585](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13382-3)

[906627](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13394-4)

[941151](#) AlmaLinux Security Update for libtiff (ALSA-2023:3711)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)