



# CVE-2022-2953

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

## Summary

<b>CVE</b>	CVE-2022-2953
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@gitlab.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-29 15:15:00 UTC
<b>Updated</b>	2023-02-23 16:01:00 UTC
<b>Description</b>	LibTIFF 4.4.0 has an out-of-bounds read in extractImageSection in tools/tiffcrop.c:6905, allowing attackers to cause a denial of service.

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Libtiff	Libtiff	All	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All

## References

Reference	Source	Link
CVE-2022-2953 LibTIFF Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>
tiffcrop: heap-buffer-overflow in extractImageSection, tiffcrop.c:6905 (#414) · Issues · libtiff / libtiff · GitLab	MISC	<a href="#">gitlab.com</a>
Debian -- Security Information -- DSA-5333-1 tiff	DEBIAN	<a href="#">www.debian.org</a>
2022/CVE-2022-2953.json · master · GitLab.org / cves · GitLab	CONFIRM	<a href="#">gitlab.com</a>
Merge branch 'tiffcrop_S-option_mutually_exclusive' into 'master' (48d6ece8) · Commits · libtiff / libtiff · GitLab	MISC	<a href="#">gitlab.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

## Vendor Comments And Credit

Discovery Credit

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

## Legacy QID Mappings

[160390](#) Oracle Enterprise Linux Security Update for libtiff (ELSA-2023-0095)

[160411](#) Oracle Enterprise Linux Security Update for libtiff (ELSA-2023-0302)

[181520](#) Debian Security Update for tiff (DSA 5333-1)

[182841](#) Debian Security Update for tiff (CVE-2022-2953)

[199019](#) Ubuntu Security Notification for LibTIFF Vulnerabilities (USN-5714-1)

[241054](#) Red Hat Update for libtiff (RHSA-2023:0095)

[241120](#) Red Hat Update for libtiff (RHSA-2023:0302)

[355148](#) Amazon Linux Security Advisory for libtiff : ALAS2023-2023-067

[502794](#) Alpine Linux Security Update for tiff

[503132](#) Alpine Linux Security Update for tiff

[505945](#) Alpine Linux Security Update for tiff

[672346](#) EulerOS Security Update for libtiff (EulerOS-SA-2022-2770)

[672388](#) EulerOS Security Update for libtiff (EulerOS-SA-2022-2735)

[672404](#) EulerOS Security Update for libtiff (EulerOS-SA-2022-2799)

[672462](#) EulerOS Security Update for libtiff (EulerOS-SA-2022-2850)

[672464](#) EulerOS Security Update for libtiff (EulerOS-SA-2022-2825)

[672772](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-1509)

[672775](#) EulerOS Security Update for compat-libtiff3 (EulerOS-SA-2023-1494)

[903774](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10779)

[903887](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10762)

[904120](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10762-1)

[904179](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10779-1)

[940871](#) AlmaLinux Security Update for libtiff (ALSA-2023:0095)

[940898](#) AlmaLinux Security Update for libtiff (ALSA-2023:0302)

[960525](#) Rocky Linux Security Update for libtiff (RLSA-2023:0302)

[960537](#) Rocky Linux Security Update for libtiff (RLSA-2023:0095)

© [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](#)**