



CVE-2022-3627

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-3627
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-21 16:15:00 UTC
Updated	2023-02-23 16:07:00 UTC
Description	LibTIFF 4.4.0 has an out-of-bounds write in _TIFFmemcpy in libtiff/tif_unix.c:346 when called from extractImageSection, to

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Libtiff	Libtiff	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All

References

Reference	Source	Link	Tags
Merge branch 'tiffcrop_fix_#411_#413' into 'master' (236b7191) · Commits · libtiff / libtiff · GitLab	MISC	gitlab.com	
tiffcrop: Heap-buffer-overflow in _TIFFmemcpy, tif_unix.c:346 (#411) · Issues · libtiff / libtiff · GitLab	MISC	gitlab.com	
October 2022 LibTIFF Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
2022/CVE-2022-3627.json · master · GitLab.org / cves · GitLab	CONFIRM	gitlab.com	
Debian -- Security Information -- DSA-5333-1 tiff	DEBIAN	www.debian.org	
[SECURITY] [DLA 3278-1] tiff security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

Vendor Comments And Credit

Discovery Credit

LEGACY: wangdw.augustus@gmail.com

Legacy QID Mappings

[160618](#) Oracle Enterprise Linux Security Update for libtiff (ELSA-2023-2340)

[160656](#) Oracle Enterprise Linux Security Update for libtiff (ELSA-2023-2883)

[181488](#) Debian Security Update for tiff (DLA 3278-1)

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

[184934](#) Debian Security Update for tiff (CVE-2022-3627)

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

[241445](#) Red Hat Update for libtiff (RHSA-2023:2340)

[241478](#) Red Hat Update for libtiff (RHSA-2023:2883)

[296098](#) Oracle Solaris 11.4 Support Repository Update (SRU) 52.132.2 Missing (CPUOCT2022)

[355865](#) Amazon Linux Security Advisory for libtiff : ALAS2-2023-2212

[355871](#) Amazon Linux Security Advisory for libtiff : ALAS2023-2023-314

[502795](#) Alpine Linux Security Update for tiff

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

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

[672478](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-1039)

[672508](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-1014)

[672526](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-1128)

[672539](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-1104)

[672592](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-1326)

[672626](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-1363)

[672651](#) EulerOS Security Update for libtiff (EulerOS-SA-2023-1391)

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

[752842](#) SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:4259-1)

[752869](#) SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:4248-1)

[904328](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (11305)

904336 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (11288)
904812 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (11305-1)
906207 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (11305-2)
906450 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (11288-2)
941030 AlmaLinux Security Update for libtiff (ALSA-2023:2340)
941082 AlmaLinux Security Update for libtiff (ALSA-2023:2883)

© [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](#)