



CVE-2022-2521

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2022-2521
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-31 16:15:00 UTC
Updated	2023-02-23 15:59:00 UTC
Description	It was found in libtiff 4.4.0rc1 that there is an invalid pointer free operation in TIFFClose() at tif_close.c:131 called by tiffcrop

Risk And Classification

Problem Types: CWE-763

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	4.4.0	rc1	All	All

References

Reference	Source	Link
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	acce
tiffcrop: free invalid pointer in TIFFClose() at tif_close.c:131 called by tiffcrop.c:2522 (#422) · Issues · libtiff / libtiff · GitLab	MISC	gitlab
Debian -- Security Information -- DSA-5333-1 tiff	DEBIAN	www
tiffcrop: -S option mutually exclusive (fixes #349, #414, #422, #423, #424) (I378) · Merge requests · libtiff / libtiff · GitLab	MISC	gitlab
2122799 – (CVE-2022-2521) CVE-2022-2521 libtiff: Invalid pointer free operation in TIFFClose() at tif_close.c	MISC	bugz
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	acce
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	acce
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.i

No vendor comments have been submitted for this CVE.

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)
182317 Debian Security Update for tiff (CVE-2022-2521)
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
355324 Amazon Linux Security Advisory for libtiff : ALAS2-2023-2055
502794 Alpine Linux Security Update for tiff
503030 Alpine Linux Security Update for tiff
503131 Alpine Linux Security Update for tiff
505944 Alpine Linux Security Update for tiff
673143 EulerOS Security Update for libtiff (EulerOS-SA-2023-2298)
673160 EulerOS Security Update for libtiff (EulerOS-SA-2023-2274)
752686 SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:3679-1)
752701 SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:3690-1)
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](#)