



CVE-2022-2867

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

Summary

CVE	CVE-2022-2867
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-17 22:15:00 UTC
Updated	2023-11-07 03:47:00 UTC
Description	libtiff's tiffcrop utility has a uint32_t underflow that can lead to out of bounds read and write. An attacker who supplies a craft

Risk And Classification

Problem Types: CWE-191

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
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Libtiff	Libtiff	All	All	All	All
Application	Libtiff	Libtiff	4.4.0	-	All	All

References

Reference	Source	Link
2118847 – (CVE-2022-2867) CVE-2022-2867 libtiff: uint32_t underflow leads to out of bounds read and write in tiffcrop.c	MISC	bugzi
Debian -- Security Information -- DSA-5333-1 tiff	DEBIAN	www.
[SECURITY] [DLA 3278-1] tiff security update	MLIST	lists.c
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

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

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

[182601](#) Debian Security Update for tiff (CVE-2022-2867)

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

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

[296086](#) Oracle Solaris 11.4 Support Repository Update (SRU) 51.132.1 Missing (CPUOCT2022)

[354109](#) Amazon Linux Security Advisory for libtiff : ALAS2-2022-1872

[354253](#) Amazon Linux Security Advisory for libtiff : ALAS-2022-1647

[502527](#) Alpine Linux Security Update for tiff

[504474](#) Alpine Linux Security Update for tiff

[672261](#) EulerOS Security Update for libtiff (EulerOS-SA-2022-2689)

[672296](#) EulerOS Security Update for libtiff (EulerOS-SA-2022-2657)

[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)

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

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

[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)

[902757](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10575) (DEPRECATED)

[902767](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10567) (DEPRECATED)

[906742](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10575-1)

[906759](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (10567-1)

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

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

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](#)