CVE-2022-3570

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-3570
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 16:02:00 UTC
Description	Multiple heap buffer overflows in tiffcrop.c utility in libtiff library Version 4.4.0 allows attacker to trigger unsafe or out of boun

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

References

Reference	Source
/tools/tiffcrop.c:8322 - Heap buffer overflow in rotateContigSamples24bits (#381) · Issues · libtiff / libtiff · GitLab	MISC
2022/CVE-2022-3570.json · master · GitLab.org / cves · GitLab	CONFIR
tools/tiffcrop.c:3142 - Heap Buffer overflow in extractContigSamples32bits (#386) · Issues · libtiff / libtiff · GitLab	MISC
Debian -- Security Information -- DSA-5333-1 tiff	DEBIAN
CVE-2022-3570 LibTIFF Vulnerability in NetApp Products | NetApp Product Security	CONFIR
tiffcrop subroutines require a larger buffer (fixes #271, #381, #386, #388, #389, #435) (bd94a9b3) · Commits · libtiff / libtiff · GitLab	MISC
[SECURITY] [DLA 3278-1] tiff security update	MLIST
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: shahchintanh@gmail.com

Legacy QID Mappings

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

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

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

184598 Debian Security Update for tiff (CVE-2022-3570)

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

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

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

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)

752996 SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:4411-1)

753515 SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2023:0060-1)

904316 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (11300)

904333 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (11283)

904356 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (11283-1)

904388 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (11300-1)

941030 AlmaLinux Security Update for libtiff (ALSA-2023:2340)

CVE.report and Source URL Uptime Status status.cve.report