CVE-2022-0907

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-0907
State	PUBLIC
Assigner	cve@gitlab.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-11 18:15:00 UTC
Updated	2023-11-07 03:41:00 UTC
Description	Unchecked Return Value to NULL Pointer Dereference in tiffcrop in libtiff 4.3.0 allows attackers to cause a denial-of-service

Risk And Classification

Problem Types: CWE-252

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	4.3.0	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora 35 Update: libtiff-4.3.0-6.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
LibTIFF: Multiple Vulnerabilities (GLSA 202210-10) — Gentoo security	GENTOO	security.gentoo.org	
2022/CVE-2022-0907.json · master · GitLab.org / cves · GitLab	CONFIRM	gitlab.com	
[SECURITY] Fedora 36 Update: libtiff-4.3.0-6.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
March 2022 LibTIFF Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
add checks for return value of limitMalloc (#392) (!314) · Merge requests · libtiff / libtiff · GitLab	MISC	gitlab.com	
tiffcrop: SEGV in _TIFFmemset, tif_unix.c:340 (#392) · Issues · libtiff / libtiff · GitLab	MISC	gitlab.com	
[SECURITY] Fedora 35 Update: libtiff-4.3.0-6.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	

[SECURITY] Fedora 36 Update: libtiff-4.3.0-6.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
Debian -- Security Information -- DSA-5108-1 tiff	DEBIAN	www.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

Vendor Comments And Credit

Discovery Credit

LEGACY: wangdw.augustus@gmail.com

Legacy QID Mappings

- 179158 Debian Security Update for tiff (DSA 5108-1)
- 184955 Debian Security Update for tiff (CVE-2022-0907)
- 198931 Ubuntu Security Notification for LibTIFF Vulnerabilities (USN-5523-2)
- 282544 Fedora Security Update for libtiff (FEDORA-2022-e2996202a0)
- 353264 Amazon Linux Security Advisory for libtiff : ALAS2-2022-1780
- 354038 Amazon Linux Security Advisory for libtiff : ALAS-2022-1625
- 354293 Amazon Linux Security Advisory for libtiff : ALAS2022-2022-049
- 354326 Amazon Linux Security Advisory for libtiff : ALAS2022-2022-194
- 354588 Amazon Linux Security Advisory for libtiff : ALAS-2022-194
- 355159 Amazon Linux Security Advisory for libtiff : ALAS2023-2023-050
- 501505 Alpine Linux Security Update for tiff
- 502035 Alpine Linux Security Update for tiff
- 502793 Alpine Linux Security Update for tiff
- 671813 EulerOS Security Update for libtiff (EulerOS-SA-2022-1869)
- 671814 EulerOS Security Update for libtiff (EulerOS-SA-2022-1845)
- 671884 EulerOS Security Update for libtiff (EulerOS-SA-2022-1937)
- 671995 EulerOS Security Update for libtiff (EulerOS-SA-2022-2161)
- 671996 EulerOS Security Update for libtiff (EulerOS-SA-2022-2136)
- 710659 Gentoo Linux LibTIFF Multiple Vulnerabilities (GLSA 202210-10)
- 900916 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (9020-1)