# CVE-2023-0799

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2023-0799 |
| **State** | PUBLIC |
| **Assigner** | cve@gitlab.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2023-02-13 23:15:00 UTC |
| **Updated** | 2023-05-30 06:16:00 UTC |
| **Description** | LibTIFF 4.4.0 has an out-of-bounds read in tiffcrop in tools/tiffcrop.c:3701, allowing attackers to cause a denial-of-service vi |

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Libtiff | Libtiff | All | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| Debian -- Security Information -- DSA-5361-1 tiff | DEBIAN | www.de |
| March 2023 LibTIFF Vulnerabilities in NetApp Products \| NetApp Product Security | CONFIRM | security |
| 2023/CVE-2023-0799.json · master · GitLab.org / cves · GitLab | CONFIRM | gitlab.c |
| [SECURITY] [DLA 3333-1] tiff security update | MLIST | lists.del |
| LibTIFF: Multiple Vulnerabilities (GLSA 202305-31) — Gentoo security | GENTOO | security |
| tiffcrop: heap-use-after-free in extractContigSamplesShifted32bits, tiffcrop.c:3701 (#494) · Issues · libtiff / libtiff · GitLab | MISC | gitlab.c |
| Merge branch 'tiffcrop_R270_fix#492' into 'master' (afaabc3e) · Commits · libtiff / libtiff · GitLab | MISC | gitlab.c |
| CVE Program record | CVE.ORG | www.cv |
| NVD vulnerability detail | NVD | nvd.nis |

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** wangdw.augustus@gmail.com

## Legacy QID Mappings

160748 Oracle Enterprise Linux Security Update for libtiff (ELSA-2023-3711)

181600 Debian Security Update for tiff (DLA 3333-1)

181682 Debian Security Update for tiff (DSA 5361-1)

183493 Debian Security Update for tiff (CVE-2023-0799)

199216 Ubuntu Security Notification for LibTIFF Vulnerabilities (USN-5923-1)

241737 Red Hat Update for libtiff (RHSA-2023:3711)

502796 Alpine Linux Security Update for tiff

503026 Alpine Linux Security Update for tiff

503134 Alpine Linux Security Update for tiff

503693 Alpine Linux Security Update for tiff

505947 Alpine Linux Security Update for tiff

672867 EulerOS Security Update for libtiff (EulerOS-SA-2023-1599)

672968 EulerOS Security Update for libtiff (EulerOS-SA-2023-1874)

672998 EulerOS Security Update for libtiff (EulerOS-SA-2023-1849)

673036 EulerOS Security Update for libtiff (EulerOS-SA-2023-1957)

673055 EulerOS Security Update for libtiff (EulerOS-SA-2023-1979)

673076 EulerOS Security Update for libtiff (EulerOS-SA-2023-2157)

673143 EulerOS Security Update for libtiff (EulerOS-SA-2023-2298)

673160 EulerOS Security Update for libtiff (EulerOS-SA-2023-2274)

710734 Gentoo Linux LibTIFF Multiple Vulnerabilities (GLSA 202305-31)

754055 SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2023:2321-1)

754062 SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2023:2334-1)

905497 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13382)

905501 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13394)

906313 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13394-1)

906516 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13394-2)

906555 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13382-1)

906585 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13382-3)

906627 Common Base Linux Mariner (CBL-Mariner) Security Update for libtiff (13394-4)

941151 AlmaLinux Security Update for libtiff (ALSA-2023:3711)