



# CVE-2019-17546

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

## Summary

<b>CVE</b>	CVE-2019-17546
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-10-14 02:15:00 UTC
<b>Updated</b>	2023-11-07 03:06:00 UTC
<b>Description</b>	tif_getimage.c in LibTIFF through 4.0.10, as used in GDAL through 3.0.1 and other products, has an integer overflow that p

## Risk And Classification

**Problem Types:** CWE-787 | CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Libtiff</a>	<a href="#">Libtiff</a>	All	All	All	All
Application	<a href="#">Libtiff</a>	<a href="#">Libtiff</a>	All	All	All	All
Application	<a href="#">Osgeo</a>	<a href="#">Gdal</a>	All	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 31 Update: libtiff-4.0.10-8.fc31 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fe</a>
RGBA interface: fix integer overflow potentially causing write heap buffer... (4bb584a3) · Commits · libtiff / libtiff · GitLab	MISC	<a href="#">gitlab.</a>
libTIFF: Multiple vulnerabilities (GLSA 202003-25) — Gentoo security	GENTOO	<a href="#">secur</a>
Bugtraq: [SECURITY] [DSA 4608-1] tiff security update	BUGTRAQ	<a href="#">seclis</a>
16443 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	<a href="#">bugs.</a>
[SECURITY] [DLA 2009-1] tiff security update	MLIST	<a href="#">lists.d</a>
[SECURITY] Fedora 30 Update: libtiff-4.0.10-8.fc30 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fe</a>
[SECURITY] [DLA 2147-1] gdal security update	MLIST	<a href="#">lists.d</a>
Internal libtiff: fix integer overflow potentially causing write heap... · OSGeo/gdal@2167403 · GitHub	MISC	<a href="#">github</a>
Debian -- Security Information -- DSA-4608-1 tiff	DEBIAN	<a href="#">www.</a>
[SECURITY] Fedora 30 Update: libtiff-4.0.10-8.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fe</a>

[SECURITY] Fedora 31 Update: libtiff-4.0.10-8.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fe</a>
Debian -- Security Information -- DSA-4670-1 tiff	DEBIAN	<a href="#">www.</a>
CVE Program record	CVE.ORG	<a href="#">www.</a>
NVD vulnerability detail	NVD	<a href="#">nvd.n</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [199525](#) Ubuntu Security Notification for LibTIFF Vulnerabilities (USN-5841-1)
- [296078](#) Oracle Solaris 11.4 Support Repository Update (SRU) 16.4.0 Missing (CPUOCT2019)
- [377286](#) Alibaba Cloud Linux Security Update for libtiff (ALINUX2-SA-2020:0130)
- [377418](#) Alibaba Cloud Linux Security Update for libtiff (ALINUX3-SA-2022:0105)
- [671104](#) EulerOS Security Update for libtiff (EulerOS-SA-2019-2707)
- [751716](#) SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:0480-1)
- [751721](#) SUSE Enterprise Linux Security Update for tiff (SUSE-SU-2022:0496-1)
- [751752](#) OpenSUSE Security Update for tiff (openSUSE-SU-2022:0480-1)
- [940309](#) AlmaLinux Security Update for libtiff (ALSA-2020:4634)
- [960802](#) Rocky Linux Security Update for libtiff (RLSA-2020:4634)

© [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](#)