



# CVE-2022-1354

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

## Summary

<b>CVE</b>	CVE-2022-1354
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-31 16:15:00 UTC
<b>Updated</b>	2023-02-23 15:50:00 UTC
<b>Description</b>	A heap buffer overflow flaw was found in Libtiffs' tiffinfo.c in TIFFReadRawDataStriped() function. This flaw allows an attack

## Risk And Classification

### Problem Types: CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
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
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All

## References

### Reference

- [2074404 – \(CVE-2022-1354\) CVE-2022-1354 libtiff: heap-buffer-overflow in TIFFReadRawDataStriped\(\) in tiffinfo.c](#)
- [heap-buffer-overflow /home/lin/libtiff/tools/tiffinfo.c:440:8 in TIFFReadRawDataStriped in branch 27f399af \(#319\) · Issues · libtiff / libtiff · GitLab](#)
- [Debian -- Security Information -- DSA-5333-1 tiff](#)
- [Red Hat Customer Portal - Access to 24x7 support and knowledge](#)
- [LibTIFF: Multiple Vulnerabilities \(GLSA 202210-10\) — Gentoo security](#)

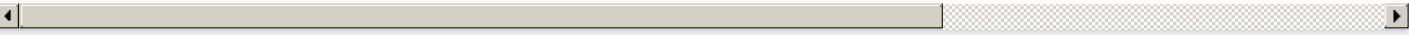
[Red Hat Customer Portal - Access to 24x7 support and knowledge](#)

[Merge branch 'fix\\_319' into 'master' \(87f580f3\) · Commits · libtiff / libtiff · GitLab](#)

[\[SECURITY\] \[DLA 3278-1\] tiff security update](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">160275</a> Oracle Enterprise Linux Security Update for libtiff (ELSA-2022-8194)
<a href="#">181488</a> Debian Security Update for tiff (DLA 3278-1)
<a href="#">181520</a> Debian Security Update for tiff (DSA 5333-1)
<a href="#">184919</a> Debian Security Update for tiff (CVE-2022-1354)
<a href="#">198944</a> Ubuntu Security Notification for LibTIFF Vulnerabilities (USN-5619-1)
<a href="#">240881</a> Red Hat Update for libtiff (RHSA-2022:8194)
<a href="#">282854</a> Fedora Security Update for libtiff (FEDORA-2022-ea3ebeff3d)
<a href="#">282867</a> Fedora Security Update for libtiff (FEDORA-2022-e9fe21d102)
<a href="#">354326</a> Amazon Linux Security Advisory for libtiff : ALAS2022-2022-194
<a href="#">354416</a> Amazon Linux Security Advisory for libtiff : ALAS2022-2022-094
<a href="#">354431</a> Amazon Linux Security Advisory for libtiff : ALAS2022-2022-183
<a href="#">354588</a> Amazon Linux Security Advisory for libtiff : ALAS-2022-194
<a href="#">355159</a> Amazon Linux Security Advisory for libtiff : ALAS2023-2023-050
<a href="#">672059</a> EulerOS Security Update for libtiff (EulerOS-SA-2022-2246)
<a href="#">672065</a> EulerOS Security Update for libtiff (EulerOS-SA-2022-2259)
<a href="#">672093</a> EulerOS Security Update for libtiff (EulerOS-SA-2022-2326)
<a href="#">672102</a> EulerOS Security Update for libtiff (EulerOS-SA-2022-2297)
<a href="#">710659</a> Gentoo Linux LibTIFF Multiple Vulnerabilities (GLSA 202210-10)
<a href="#">940811</a> AlmaLinux Security Update for libtiff (ALSA-2022:8194)

© [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](#)**